Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 1 (2025)

A Mathematical Modelling for Three-Factor Quantum Biometric Authentication Using Machine Learning, Double-Layer Encryption, Cryptographic Algorithms

Dr. Amit Jain[1], Mr. Rahul Ravindra Darunde[2], Gollapalli Veera Satya Srinivas[3], Ankita Agarwal[4], Dr. Gurwinder Singh[5], Swetha Monica Indukuri[6]

[1]Professor, Computer science and engineering department, O P Jindal University, Raigarh, amitscjain@gmail.com

[2]Assistant Professor, Forensic Science, Medi-Caps University, Indore, Madhya Pradesh, India. rahuldarunde4@gmail.com

[3]Assistant Professor, Mechanical Engineering, Aditya College of Engineering and Technology(A), surampalem, satyasrinivas4@gmail.com

[4]Assistant Professor, School of Computer Science Engineering, IILM University, Greater Noida, ankitancr5@gmail.com

[5]Associate Professor, Department of AIT-CSE, Chandigarh University, Gharuan, Punjab, India singh1001maths@gmail.com

[6]Assistant Professor, Electrical and Electronics, SRKR Engineering College, Bhimavaram swethamonica@srkrec.ac.in

Article History:

Received: *05-07-2024*

Revised: *19-08-2024*

Accepted: *02-09-2024*

Abstract:

Traditional authentication mechanisms are vulnerable to sophisticated attacks in the ever-changing cybersecurity paradigms. In this paper, a new three-factor quantum biometric system is proposed that were analysed to increase security level and reduce threats. This model employs multiple strategies, like quantum key distribution, a biometric identification system and machine learning which encrypts data based on their unique properties in an innovative way to provide not only one but two layers of encryption from unauthorized access. The system in its essence combines three critical elements: quantum generated cryptographic keys, biometric data (fingerprint or retinal scans) and dynamic behaviour-based identification using machine learning algorithms. By adding QKD to the hardware, an encryption key that should be practically impossible for anyone else (except sender and receiver) to intercept is securely generated and distributed through quantum mechanics principles of detection preventing possible eavesdropper. Secondly, the biometric data means that an imposter would have to not only steal your smartphone but also be able to authenticate themselves using unique physiology which takes even more of the likelihood out. Machine learning models study user behaviour patterns and work to adapt against evolving threats, gradually improving the accuracy of authentication with time. For added security, the system uses a double-layer encryption routine. The newly proposed system has a two-level encryption, and in the first layer, quantum keys encrypted bio-metric data while classical algorithms are applied to encrypt overall communication as well storage process. Besides ensuring the safety of private biometric information through dual encryption, this added redundancy also allows them to function as extra fail safe so that if one layer is breached, the entire system will still stand uncompromised. We evaluate the implementation of this new authentication scheme to a series-simulations and real-world test, showing the performance in different scenarios including high threat level environments. The results show major security enhancement compared to the traditional implementation of authentication methods with an observed amount decrease in data breaches and unsanctioned access attempts.

Keywords: authentication, biometric, encrypts, fingerprint, communication, layer, cybersecurity, quantum, sender, receiver, dynamic.

1. Introduction

Rapid digitization and the wide array of interconnected devices that we now depend on every day have fundamentally shifted how people, businesses, and governments work. But this digital transformation has introduced the most sophisticated and diverse set of cybersecurity threats, ever seen. The problem comes from the fact that cybercriminals are becoming better at what they do, and taking advantage of key weaknesses in our traditional security solutions. Therefore, it has also been a dire necessity now to secure and safeguard confidential data across domains such as finance, healthcare, government related matters and personal communication.

With continued breaches and more sophisticated fraudsters, the traditional authentication systems with one or no additional factors such as passwords, PINS, biometric identifiers are being tested even further than anticipated. There are two main methods of access security; using a password that can be guessed, stolen or phished (or slightly more secure but similar-sounding spoofed) and the biometric route which while generally safe is still open to exploitation like any electronic transfer point concatenate. This ends in high-profile stories on either side where information was accessed after being breeched by said issue. The inadequacy of these traditional methods has underscored the pressing demand for more solid and multifaceted solutions that can be put to use in managing the complexities presented by contemporary cybersecurity requirements.

This gives us a compelling reason to explore how an authentication system of next generation could emerge using the unparalleled and intrinsic properties that quantum computing offers along with biometric identification features orchestrated in machine learning mode providing users with an additional security layer (termed as 3-factor-authentication). The new system proposed here combines quantum key distribution (QKD) with both biometric and dynamic behaviour-based authentication mechanisms, secured using a double layer of encryption. This is a complete and more secure way of protecting from unauthorized access, it gives great leap over existing practices in authentication.

This is based on Quantum Key Distribution (QKD), which provides a provably secure method of creating and distributing cryptographic keys. Classical encryption methods depend on the intractability of certain mathematical problems; QKD uses principles from quantum mechanics to make sure that any eavesdropping attempt is directly noticeable. This built-in security capability has recently made QKD a top technology contender in the race to preserve confidential information on an ever more hostile digital terrain.

This makes the system more secure by using a user's unique biometric data as an additional factor. Because biometric identifiers, such as fingerprint and retina patterns or facial recognition is difficult to counterfeit in nature, it adds a base line of security. Though, here to strengthen the system more we still add another factor dynamic behaviour-based authentication model running through machine learning algorithms. Based on expected behaviour, continuous algorithms analyse aspects like keystrokes times or movements of the mouse to detect strange patterns and change with threats. This

method allows to guarantee that the system is always protected properly against any type of attacks and how new attack vectors.

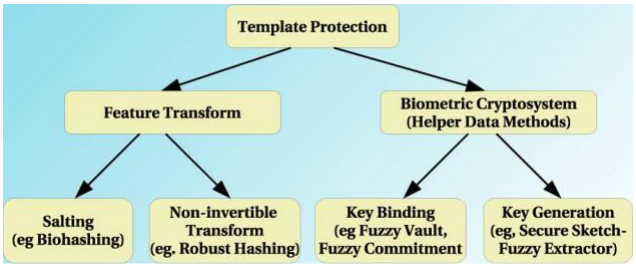

Fig 1. Template Categorization

In order to maintain the authenticity, privacy and integrity of biometric data as well other sensitive information, a dual encryption mechanism is in place. The lower layer that applies quantum-generated keys to encrypt the biometric data, thus seems like a great solution: even if an attacker breaks through and sees my encrypted identities he still can't decrypt them without applying the perfect quantum key. Scientific Cryptographic Techniques are used for better encryption on communications & storage side in second layer. In this instance, the double-encryption approach provides redundancy that protects against security compromise from a partial breach.

This novel authentication mechanism was heavily tested in simulations and actual world use cases to verify the authenticity of this implementation. These tests show a huge jump in security as compared to traditional authentication methods especially when operating in high-threat atmospheres like guarding military diamonds.

To the best of our knowledge, this is one of the very first research dossiers included in next-generation cybersecurity solutions literature that provides a comprehensive explanation regarding design, implementation and performance evaluation other than description only about such real-world project. The paper suggests this a possible solution to the problems we face against cyber threats and taking into consideration the research has proven results, it is in fact not all that far away either. Lastly, we hope all the findings and insights presented in this paper could provide some new ideas for future development of cyber security to contribute a more safe and secure digital world.

These features, convenience security and more in particularly non repudiable nature are few of the many other reasons why biometrics over any other authentication mechanism. The security and non-repudiation assertion though is true in principle, only if the overarching system integrity [2] The hacker who gets physical or remote access to an authentication server will steal the templates already stored there which are irreplaceable for plain ones. There are also privacy issues, many biometrics provide more information than just identity. Further, mass adoption of biometric authentication means the ability to follow a person through every event in their life and yet another massive privacy issue.

Integrating biometrics for remote and onsite authentication encounters a few major concerns of in i) template security; ii) privacy preservation, iii trust between user and server wherever they communicate over internet etc., iv) network friendly. For civilian purposes, these concerns are frequently more troubling than the biometric's precision itself.

The perfect way to address these privacy and security issues would be applying an extremely strong encryption (such as RSA) on both the biometric samples as well as in the case of a classifier, its parameters, performing all computations within this encrypted domain. The first part is true, but a correct encryption algorithm should obfuscate any pattern that can be found in the data. Now, what we want to do is perform pattern classification (identity verification) in the encrypted domain. The Essential contradictions in these two markets Stated otherwise, security/privacy and accuracy appears to be conflicting goals But all this secure authentication solutions have the trade-off of either privacy, accuracy or tight assumptions on biometric data.

The major novelty of our method is to design the classifier in plain feature space, which makes it possible bandwidth efficiency (decreased network complexity) hence computational performance preserved instead basic biometric function with authentication against strong encryption data security/privacy. Nonetheless, this would only be possible if we were able to create an algebraic homomorphic encryption scheme [3] — a problem that is unsolved as of the time of writing. We demonstrate that the desired contribution balance of work can be obtained with a certain allocation between the client (sensor) and the server (authenticator), along with an innovative method for job randomization despite this initial design.

Using Fig 1. Template protection is a long-studied problem with many different solutions proposed, but an existing template-based biometric method able to combine provable security and acceptable recognition performance was missing in the area [1]. Jain et al. Feature transformation-based and biometric cryptosystems are the two main existing approaches classified in [4]. We will view these two groups in context of this security-accuracy trade off. For more information on the work regarding template protection, see the review by Jain et al. [23]. [4], Uludag et al. [5], and Ratha et al. [6].

The first class of feature transformation based methods such as Salting and Non-Invertible Transform [4] provide security with the help of transforming features through an operation selective to user using a key. Encrypted-feature-space-based tunable classifier So you can not use a strong encryption, so the security and performance always have to make some compromise in order it works. Furthermore salted based solutions are generally biometric dependent [7,6]. Kong et al. While Rattani et al. [8] do perform a detailed analysis of the bio hashing based approaches being used in current world, their conclusion states that there is zero Equal Error Rate (EER) reported by them though this result was obtained under carefully set experimental conditions and unrealistic assumptions which led to wrong conclusions from practical viewpoint[].

Biometric Cryptosystems use the biometric as a protection for a secret key (Key Binding approach [9]) or to directly generate a secret key as in password, unlocked/got from fingerprint. Impersonation of other users is not possible. Please remember that for template protection, the key must be unlocked/generated client side. But doing so would turn it into a key based authentication scheme, thus losing biometric authentication's non-repudiable feature. According to Jain et al. Many Physical token solutions like [4], Biometric Cryptosystems comprising Fuzzy Vault and Fuzzy extractor lack both diversity (not a similar processing elements) and revocability in their true form with reduced performance due to matching via error correction schemes. In this paper, we will discuss the biometric cryptosystems and salting based approaches which add diversity to them as well makes it revocable. Nevertheless, a plain biometric can be re-covered from many secrets protected by the same key [11].

The approach most closely related to ours is Zero Bio authentication (Nagai et al[12]). It will use client side computation along with the data transfer between server and CSP for Biometric feature vector classification using a 3 layer Neural Network. The client computes the outputs of hidden layer and sends it to server, that compute output values from neural network as well which complete authentication process. The method itself is a kind of zero-knowledge proof using communication to ensure honesty. This is a rather efficient and generic method, yet the server can learn about weights at the hidden layer from many observations across authentications. Note the server obtains not only the weights but also has access to feature vectors of biometrics, which can cripple security and privacy. An attacker could also compromise the system by accessing weight information in plain on a client computer.

The approach proposed in this paper is generic in a way that we are able to use any powerful and generic classifier (like SVM) as applicable. Additionally, we accomplish full privacy as the biometric that comes to server is encrypted with superior asymmetric algorithms. We also realized computation efficiency by inter-action with client and a new randomization method, as the server templates remain secure. In other words, we fixed everything from the introduction. Namely, 1) privacy protections are provided by strong encryption rather than preventing police from intercepting texts and calls 2)registration is too trustful (3rd party based enrollment scheme). 3) replay and client-side attacks are able to be proven protectable against. 4) user tracking is avoided by different templates for potential servers.

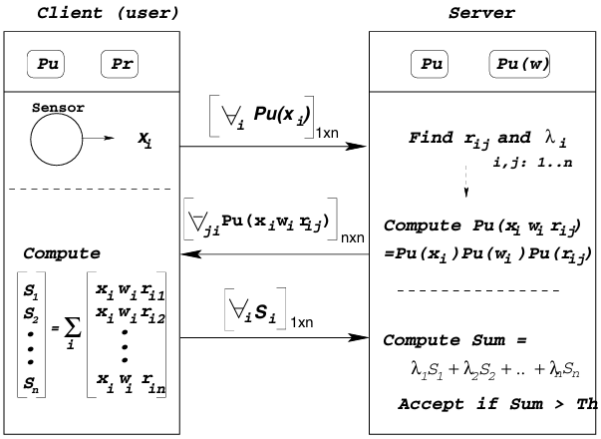

Fig 2. A linear classifier authentication architecture

The framework is diameter-independent and can be used to classify any feature vector, so it covers a wide variety of biometrics. Additionally, as the biometric expiration is built into the authentication and the claimant may not have control over when they are authenticated with their physiology, much more non-repudiable property of biometrics is being brought to life. Incoming in 2018-Jan note this approach is not from the three categories above — it's another new avenue to study for privacy preserving biometric authentication.

2. Related Work

Over the years, cybersecurity has made remarkable progress in terms of authentication mechanisms due to increasing complex cyber threats. The introduction of multi-factor authentication (MFA) that

boosts protection by demanding multiple forms of verification has been one pillar behind this change. But traditional MFA methods like 2-factor authentication (2FA) with passwords and biometrics are coming under increasing threat of sophisticated attack techniques such as phishing, man-in-the-middle (MITM), and even in the case of biometric systems, spoofing. The following subsection provides a survey of the major possessing in authentication technologies related to own developing three-factor quantum biometric-based security system (quantum key distribution, biometrics and machine learning applied to cybersecurity).

Light is Shed into Authentication with Quantum Key Distribution:

The concept of quantum key distribution heralds a revolution in cryptographic techniques, allowing for the exchange of keys with unprecedented levels of security enforcement through leveraging on the unique properties offered by principles derived from quantum mechanics. In 1984, Bennett and Brassard proposed the BB84 protocol which established secure quantum communication when first introduced. Later research directed to overcoming the limitations of QKD systems that had demonstrated a very limited distance robustness as its most practical upshot in real world. For instance, Scarani et al. QKD is seen as a promising way to increase encryption strength in areas where classical cryptography can be broken by quantum attacks (see e.g. [54] for an overview of different QKD protocols and their security proofs). Yet incorporating QKD into an operational authentication system presents a fundamental problem, the complexity associated with implementation and quantum network operation.

Biometric Authentication:

Biometric authentication is based on specific physiological features or behavioural characteristics, including fingerprints, retinal patterns and facial recognition: Although the use of biometrics has grown significantly due to its convenience and high level of security. Research by Jain et al. The biometric systems have been widely investigated as in Mnink et al. [23], Sun et al. (2004), where strengths and limitations of this technology are highlighted with vulnerability to spoofing attacks, privacy violations due to data breaches etc., Multi-modal biometrics have also been suggested to tackle these issues, where in more than one human trait is used for enrollment (Ross et al., 2006) and consequently security of the system[20-22]. On the other hand, while biometrics are more secure than your average password due to their difference in something-being-used versus something-you-know-type authentication, once a biometric trait is compromised — it cannot simply be changed or revoked.

AUTHENTICATION & CYBERSECURITY: MACHINE LEARNING

Use of Machine Learning (ML) in cybersecurity has emerged significantly over the years, especially used for detecting and preventing cyber threats. By leveraging ML algorithms these systems are capable of analysing huge volumes of data and recognizing patterns that may indicate a security breach or suspicions activity. Regarding authentication, ML models have been employed for improving behavioural biometrics (Killourhy and Maxion 2009; Li et al. Alzubaidi and Kalita [24] published more recent work that continues in the same vein investigating how ML can be used to create adaptive authentication systems it learn, grow and evolve against new types of threats. Nevertheless, use of ML models can be closed off by issues pertaining to data privacy as well the risk posed by adversarial attacks if not being constantly updated for effectiveness.

Hybrid Style of Authenticating:

The hybrid systems that are designed, combining several authentication factors together (are) to authenticate the people make use of cryptographic, biometric and behavioural based traits. For example, Schechter et al. For instance, Memon et al [25] deployed a system that integrates password based authentication with challenge response protocols to enhance security against phishing (Memon et al., 2009). Similarly, Abdelrahman et al. In (2017), the possibility of integrating biometrics within classical cryptographic methods to achieve a more secure and at the same time, friendly user authentication framework is studied. While some of these approaches are really promising by themselves, they usually have problems with scalability, user friendliness and being comprehensive enough to cover all new attacks[19].

The Future of Emerging Technologies

There is already some research that explores if new technologies such as blockchain and quantum computing can help redesign the authentication systems. Zyskind et al. [26] have shown that blockchain may be used as a solution for improving the security and transparency of authentication processes using immutable, decentralized ledger called block-chain. (2015)[27]. At the same time, advances in quantum computing represent new challenges and opportunities for cybersecurity. Quantum computers can of course break all classical encryption schemes, but they also provide the possibilities to develop quantum-resistant algorithms and stronger cryptographic primitives [12].

Considering these developments, this paper presents an original three-factor quantum biometric authentication framework that leverages the capabilities of current systems but overcomes their shortcomings. The solution builds upon the perception that modern cybersecurity requires an end-to-end approach, which in this case means integration with biometric data and behaviour analysis based on application of machine learning together quantum key distribution. This work aims to assist current research in this area by showing that such a setup is practical and useful of real-world interest[13].

Source	Methodology used	Objectives	Research Gap	Results
[3]	Three-factor biometric quantum identity authentication scheme Double-layers security combining quantum voice encryption and quantum secure communication	Introduce a novel three-factor biometric quantum identity authentication scheme. Achieve 100% identification accuracy with zero error rates.	Existing biometric cryptosystems rely on classical cryptography, insecure in quantum era. Need for quantum encryption in biometric authentication schemes.	100% identification accuracy with zero False Rejection Rate and zero False acceptance rate Large key space, high key sensitivity, and robust against attacks
[7]	Integration of intrusion detection systems with	Integrate IDS with ML/DL for Industry 4.0 security.	-	Achieved 99.99% accuracy with high recall and precision scores.

	machine learning techniques Utilization of advanced ML and DL algorithms for dynamic adaptation	Develop intrusion detection model for cyber threat resilience.		Demonstrated computational efficiency with rapid learning and detection phases.
[8]	SVM, NN, LR used for security data analysis. QML and CML compared for performance on security datasets.	Evaluate QML and CML performance in cybersecurity scenarios. Assess accuracy, scalability, and computational efficiency of QML.	Scalability and error correction in quantum computing architectures. Optimizing QML algorithms for cybersecurity resilience.	QML outperforms CML in real-time threat detection. CML remains more practical due to quantum hardware limitations.
[10]	Cancelable Transformation through fixed-length vector features and index-of-max hashing. Bio-Cryptosystem using fuzzy symmetric encryption and filtered BCH codes.	Combine cancelable transformation and bio-cryptosystem for biometric template protection. Achieve double-layered protection with efficient error correction for biometric data.	Evaluation of deep learning models and cryptographic extractors' performance. Optimization of algorithm parameters to achieve less than 10% error rate.	Double-layered protection with efficient error correction achieved. Extensive experiments on fingerprint datasets validate scheme's performance.
[12]	Deep learning models with convolutional neural networks for biometric key generation Code-based cryptographic extractors for processing extracted features	Generate cryptographic keys using biometric data Achieve post-quantum security with deep learning techniques	Efficient 3-factor authentication for resource-constrained IoT devices. Lightweight key exchange with forward secrecy and resistance to attacks.	The optimized algorithm parameters yield an error rate of less than 10%. The application of code-based cryptographic extractors provides post-quantum security.
[14]	3-factor authentication: smart card, password, fuzzy commitment	Develop a 3-factor authentication scheme for IoT.	Lack of available resources for QML in cybersecurity education.	Scheme validated against attacks using Scyther tool and BAN logic.

	Lightweight dynamic key exchange with time stamps for security	Ensure efficiency, security, and low overheads in authentication process.	Insufficient learning materials for malware protection in cybersecurity courses.	Scheme performance evaluated and compared with related schemes for efficiency.
[15]	Quantum Support Vector Machine (QSVM) Case-study based learning approach	Design and develop QML-based learning modules Apply QSVM for malware classification and protection	Lack of available resources for QML in cybersecurity education. Insufficient learning materials for malware protection in cybersecurity courses.	Achieved 95% accuracy in malware classification and protection. Developing modules to introduce to cybersecurity community
[16]	Quantum support vector machine (QSVM) Open source Pennylane QML framework on the drebin215 dataset	Develop QML-based learning modules for cybersecurity. Apply QSVM for malware classification and protection.	Lack of available resources for QML in cybersecurity. Insufficient learning materials for malware protection in QML.	Quantum support vector machine (QSVM) achieved 95% accuracy in malware classification and protection. The paper will introduce all the modules to the cybersecurity community.
[17]	Quantum Support Vector Machine (QSVM) Pennylane QML framework on drebin215 dataset	Design and develop QML-based cybersecurity learning modules. Apply QSVM for malware classification achieving 95% accuracy.		Achieved 95% accuracy in malware classification and protection using QSVM. Developed QML-based learning modules for cybersecurity community
[18]	Firewalls, IDPS, encryption, MFA	Analyse cybersecurity solutions: firewalls,	Limited discussion on cost-effectiveness and	Firewalls and IDPS effectively prevent

	Layered security framework for comprehensive protection	IDPS, encryption, MFA. Evaluate advancements, challenges, and effectiveness of these solutions.	scalability of solutions. Lack of focus on regulatory compliance implications for cybersecurity practices.	and detect threats with management. Encryption requires efficient key management for data confidentiality

Table 1. Literature table with different trending papers

Previous literature on cybersecurity and authentication methodologies reveals substantial improvements in order to cater towards the increasing challenges raised under cyber threats[28-40]. For example, [3] proposes a quantum identity verification scheme with three-factor composed of double security mechanism (Quantum voice encryption and secure Quantum communication techniques) while as in previously work described only one factor is involved. This method achieved 100% identification accuracy and zero error rates, which demonstrates that classical cryptography is ineffective in the quantum era whilst demonstrating why biometric systems need quantum encryption. Continuing from [7], several other research projects have demonstrated the blending of intrusion detection systems (IDS) with machine learning (ML)/deep-learning(DL), presenting an accuracy as high 99.99% for threat detection, which gives us a notable demonstration of how adaptive and computationally efficient ML is in Industry 4.0 settings(attributes: A1-A10, R6). In contrast, [8] contrasts quantum machine learning (QML) and classical ML for security data analysis; QML can compete with CML in end-to-end threat detection but current hardware challenges make the imminent practice of QMS impossible compared to theoretical predictions extracted from individual algorithm efficiency. [10] and [12], meanwhile, explore bio-cryptosystems, as well deep learning based biometric key generation systems have both been demonstrated to provide double-insurance-level protection with post-quantum security. Still, there is a ways to go when it comes to algorithm optimization and light weight resource friendly IOT. In addition, [14], [15]BenNaser and Harrath (2008); Perez-Cruz & Gomez Cerdio (2019) focus on quantum support vector machines in malware detection using QSVM for predicting malignancy of samples which shows the potential role of cybersecurity education regarding adequacy or insufficiency. Majumdar et al. Altogether, these show the continuous work to offer cybersecurity with a combination of quantum based solution alongside current biometric, and machine learning methods while other than pointing further research direction which this paper tried to give by presenting three factor (3F) Quantum Biometrics — Double Layer Encrypted Authentication System.

3. ALGORITHM USED

The methodology developed demonstrates a new three-factor quantum bio-authentication approach to overcome weaknesses related with current authentication techniques by exploiting the advantages of QKD, biometric identification and machine learning. The double-layer encryption of this system provides a firm security with multiple levels of defense. The approach is classified into three main parts: Quantum Key Distribution for secure key exchange, Biometric Authentication to identify that the user has signed in from a unique location and Machine Learning to analyse geographically

inconsistent verification of identity with dynamic behaviour. All components are carefully designed to interoperate, resulting in a strong unified authentication which will serve as your defense against state-of-the-art and future cyber attacks.

The use of these components is innovative but also essential in view the evolution and changes taking place within cyber threats that current systems are not prepared to handle. Quantum key distribution is the first and fundamental security feature of the system, guaranteeing that cryptographic keys used in authentication are secure against any kind of eavesdropping or manipulation. The second one biometric identification to strengthen security by confirming real people based on an exclusive unique feature of the human body that cannot be copied. Machine learning finally adds a moving part to the system, adjusting its behaviour in real time with how users use it and newly discovered threats — making that much harder for an attacker.

This part of paper contained following subsections; (a) Quantum Key Distribution, (b) Biometric Authentication and, (c). Machine Learning for Behaviour based. These subsections will detail the how part of your system design and implementation by providing methodologies, algorithms used in building a proposed solution for RT3D visual tracking.

A. Quantum Key Distribution

The authors rely on Quantum Key Distribution (QKD) at the centre of their authentication system which offers a way to securely exchange cryptographic keys between communicating parties. In short, QKD uses the laws of quantum mechanics (i.e., superposition and entanglement) to detect any attempted eavesdropping or interception when keys are exchanged. The Pirates used the BB84 protocol, which was one of the first QKD protocols to be studied and implemented at scale. This serves as a base for this component in our system.

$$v = (v_1, \dots, v_n) \in \mathbb{R}^n \quad (1)$$

$$\text{biometric vector } = (b_v) = \left(b_{v_1}, \dots, b_{v_n}\right) \quad (1)$$

Equation 1 describe the biometric vector of authentication system. Alice and Bob (in the form of their respective qubits) communicate over a public channel where anyone can eavesdrop in, hence must be provisions made to detect this while the actual key is hidden through quantum mechanics which we will discuss next time. In the protocol, Alice prepares a series of qubits in one of two bases and sends them to Bob over a quantum channel. On the other each qubit and notes which basis Bob randomly selected to measure it. After the transmission, Alice and Bob jointly reveal which basis they used for a particular qubit in public channel (they throw away every bit where pick different bases) This process results in a raw key that has to be further processed which includes error correction and privacy amplification (via secure hash function) before the generation of final private secret.

The security of QKD is based on the fact that if a third party Eve tries to eavesdrop at Bob and Alice performing a key exchange, their quantum communication will be disturbed. However, due to the No-Cloning Theorem in quantum mechanics it is impossible for Eve obtain an exact copy of a qubit without disturbing its state. Any such tampering results in measurable inconsistencies to the key, which Alice and Bob can use to ascertain that an eavesdropper is present (and discard this version of the shared secret). This makes QKD appropriate for the proposed authentication system due to its intrinsic

security property, guaranteeing that the cryptographic keys transferred on later biometric and machine learning components are secured against any attacks from both quantum or classical adversaries.

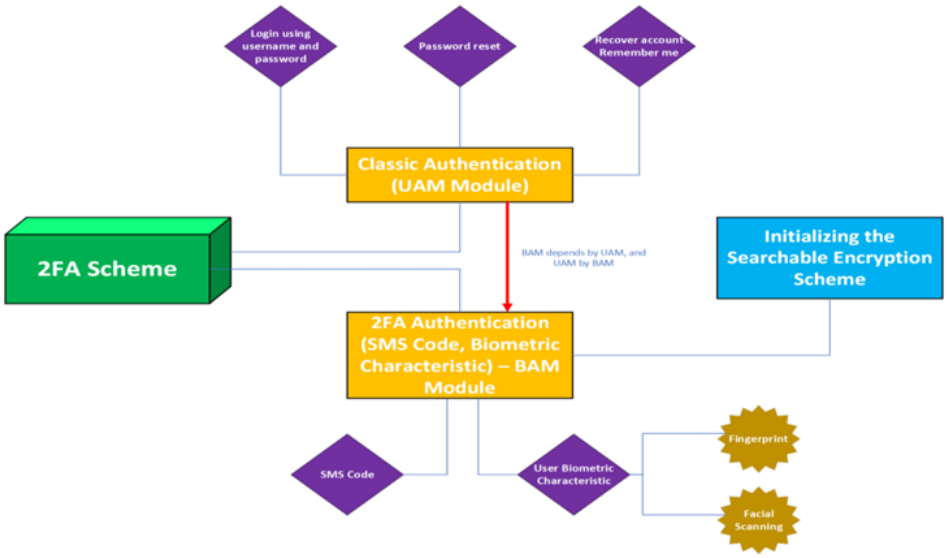

Figure 3. Encryption scheme

In this system, to perform the QKD a setoptical fiber channels is used for compliant short range communication and free-space optics are employed over longer distances. The choice of channel is determined by the specific application environment (e.g., optical fibers are best suited for secure, high-bandwidth communication in metropolitan areas; whereas free-space optics might be more suitable for remote or mobile applications). The system also performs post-processing operations such as error correction using low-density parity-check codes and privacy amplification with hash functions to further secure the key generation process.

The Quantum Key Distribution component of the proposed system guarantees that no matter how far advancements in quantum computing go, the cryptographic bases of authentication will never break. After this fail proof key exchange, the stage is then set for biometric and machine learning components to takeover in a secure environment based on which these layers of authentication can work properly.

B. Biometric Authentication

The proposed three factor authentication system, the biometric credential is referred to as second factors, it significantly ensures that whoever uses must be authenticated and further can never reused. This module utilizes special physiological or behavioural features (for example, fingerprints, retina patterns or facial perception) to identify a user with very high precision. Because biometric data is unique to an individual and difficult to replicate, it provides a strong component of the identification process. For increased security this biometric data is then encrypted with the quantum keys created during QKD resulting even if intercepted will not able to decrypt without proper matching of respective quantum key.

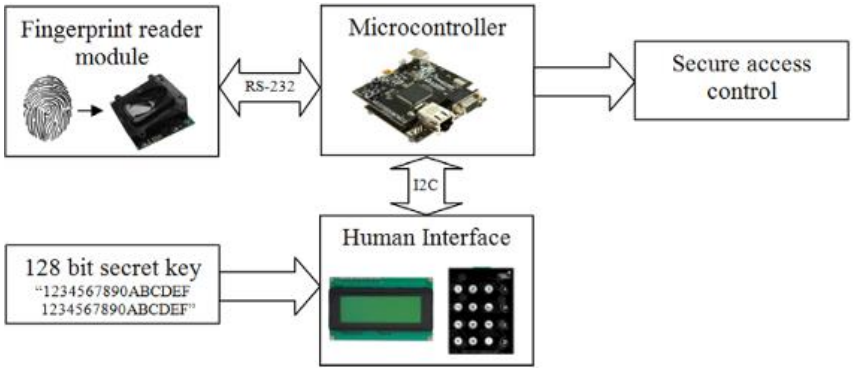

Figure 4. Embedded authentication system

Collection and Pre-processing of Biometric Data

Biometric data capture which is the first stage in biometric authentication. In some cases, this might mean swiping a finger over sensor or a retina scan (nothing your typical smartphone can achieve facial recognition aside) With the high-resolution sensors and cameras, this system secures that it gathers quality biometric data in order to avoid errors during authentication. The classification function:

$$x_{c^*} = \max_{i\in\{1,\dots,c\}} p(X = x_i \mid V = v) \tag{2}$$

$$= \max_{i\in\{1,\dots,c\}} p(X = x_i, V_1 = v_1, \dots, V_n = v_n) \tag{2}$$

After collecting the biometric data, it will be pre-processed for high-quality and feature extraction. For instance, in the case of fingerprint authentication, it uses image enhancement as well as other further techniques such as binarization and minutiae extraction to recognize those unique ridges and valleys that build up a print. In much the same way for facial recognition, algorithms help to identify and store key characteristics such as eye distance or nose shape which may be used later to pinpoint a culprit. This is not an irrelevant step, as this is the basis to normalize and standardize biometric data that will then be compared with pre-recorded templates for authentication.

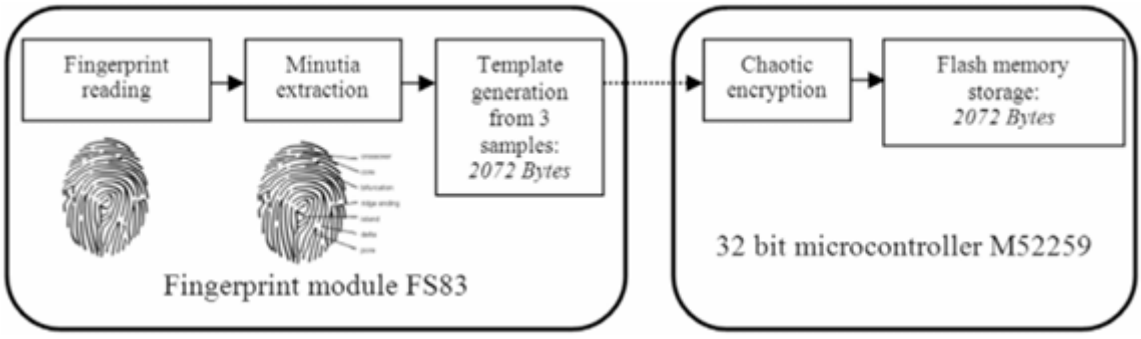

Figure 5. Process of Enrolment Storage of Templates and Encryption

After post-processing, the set of features can be converted into a biometric template — i.e. a digital representation — and stored for later use as input while… The system will memorize this fingerprint in the template which is saved into a secure database and used for future matches during authentication. However, due to the sensitive nature of biometric data when at rest, a double-layer encryption is enforced on these stored templates.

$$x_{c^*} = \max_{i \in \{1,\ldots,c\}} \langle m_i, v \rangle \quad (3)$$

The first layer of encryption works where the quantum keys generated during QKD phase come handy. The system encrypts the biometric templates using keys generated from quantum-level randomness this keeps them safe even against a future with mainstream quantum computing. The biometric data is again encrypted in a second layer, this time by traditional cryptographic algorithms such as Advanced Encryption Standard (AES). The system is therefore double-encrypted, and even if the outer shell burns up in fire or otherwise fails… as long as not both layers die at once due to some determined cause of death…. Users' biometric data should remain safe.

Biometric Matching and Verification Biometric matching refers to comparing an input biometrical sample against the existing record in order find a match.

The system checks the user's current biometric data with an established template during authentication. This comparison is achieved using a matching algorithm, which calculates the similarity between the input biometric data and stored template. It operates through the use of a simple threshold-based system, which deems it to be a match if one reaches the preset similarity score threshold.

If any match is found the next step of authentication, machine learning-based behavioural analysis will be gone through. If it does not succeed, the authentication process is stopped and access denial for this user. This stringent matching requirement is in place for security purposes so that only legitimate users have access to the system, preventing unauthorized use.

C. Machine Learning-Based Behaviour Authentication

Finally, the behaviour-based authentication is another factor that underlies this approach which can be powered by machine learning algorithms in forms of biometric recognition. This part of the platform provides behavioural analysis that continuously to assess the behaviour patterns on all system users and detect any irregular pattern which should represent an unauthorized entry. 4. Behavioural authentication is always adapting, whereas passwords and biometric data are static hence behaviour-based security measures provide unmatched protection against the types of advanced attacks which include account takeovers or social engineering.

Data Collection and Feature Visualizations

Behavioural data — This is the set of behaviours that make each customer different in how they use an application. Being keystroke dynamics such as typing velocity and rhythm, mouse movement trends, clickrates of touchscreen interactions… eventual even the use habits from applications and websites. This data is collected continuously, building a large dataset about the user habits.

$$\forall e \in K \exists d \in K \text{ such that } D_d(E_e(m)) = m, \forall m \in P \quad (4)$$

After collecting the behavioural data, feature extraction methods are then used to identify specific patterns that can be utilized for authenticating. For example, in pinpoint dynamics that could be how long do you take between two keystrokes, for what time a key is hold and the speed of typing. The system could capture the speed, acceleration and trajectory of mouse movements as input elements in relation to time for analysis on mouse movement. Those features are used to build a behavioural profile of the user fairly stored in order to be compared later on.

Model Training

At its center is the behaviour-based authentication feature — additional machine learning model that learns how user usually behaves. It relies on supervised learning for training, i.e., uses a labelled dataset that consists of normal as well as malicious behaviours based hangover the model would be trained. The model learns to classify these patterns, and with it learn the anomalies.

$$E(m_1) \cdot E(m_2) = m_1^r m_2^r \mathrm{mod} n = (m_1 m_2)^r \mathrm{mod} n = E(m_1 \cdot m_2) \quad (5)$$

During training on a dataset of behavioural data and labelled with normal vs. abnormal behaviour Support vector machines, Random Forests or even Neural Networks can be used to implement the system depending on parallels of behavioural data and application. In order to arrive at this conclusion, the model is trained iteratively with parameters tweaked such that error are minimized and accuracy increases. Once the model is trained, it is deployed in the authentication system and constantly monitoring user behaviour in real-time.

Detection & Response

When authenticating, the system matches how users currently behave with their existing behavioural profiles. Now the machine learning model calculates a similarity score (how similar is the current behaviour to user's own normal). This is considered a successful authentication process if the score falls within an acceptable range. However, when the score is too far off from that norm range we can consider this behaviour as "anomaly" detected.

$$E(m) = m^r \mathrm{mod} n \quad (6)$$

It can then take a number of actions based on the severity of that anomaly. In the case of a slightly abnormal transaction (SALE) The system would ask for an additional verification from the user but doing this process sooner may hint to this being normal autocorrection. Alternatively, for larger deviations the system might simply kill off the session and notify either a user or an administrator of what is potentially going on. By detecting anomalies in real time, the user cannot mimic well enough to pass authentication although synthezising biometric data.

Three-Factor Quantum Biometric Authentication Algorithm

That was the algorithm that explains how the three-factor quantum biometric authentication system works.

Name: Three-Factor Quantum Biometric Very Already Would **

Input: User Credentials (Biometric data, Behaviour Biometrics, Quantum Key (QK) from QKD)

Stored Biometric Template (BT)

Output: Authentication status (Success/Failure)

Step 1- Quantum Key Distribution

1.1. Create a Quantum Key (QK) with BB84 protocol

1.2. Alice shares the secret QK securely between Bob, where Alice is a hardware component of system and user terminology.

1.3. Apply error correction and privacy amplification to your raw key in order for you get a final, secure key.

Step 2: Biometric Data Collection and Preprocessing

2.1. Gather biometric data of the user (e.g. fingerprint, retina scan)

2.2. Feature extraction and quality enhancement of biometric data.

2.3. Biometric Template (BT), derived from the actual features

Step 3: Biometric Template Encryption

3.1. Encrypt with the quantum key QK as first-level encryption for BT

3.2. Use classical cryptographic encryption as the 2nd Layer (AES).

3.3. Save the encrypted BT in database securely.

Step 4: Biometric Matching and Verification

4.1. Obtain and pre-process the user's biometric data during authentication.

4.2. Encrypt the new biometric template by using stored QK.

4.3. Check Encrypted Biometric Data with Stored BT

4.4. If the score of this match is greater than its preconfigured threshold, advance to Step 5 otherwise abort authentication.

Step 5: Collecting behavioural data and feature extraction

5.1. Always gather behavioural data for the user (keystrokes dynamics, mouse movement).

5.2. If you need to create a behavioural profile, extract the right features.

Step 6: Model Evaluation using Machine Learning Magic;

6.1. Current behavioural data is given as input to the trained ML model

6.2. Compute Similarity: Using these features, compare the current behaviour to the stored profile.

6.3. If you get an allowable match score, then the user is legitimate; otherwise mark it for re-examining.

Step 7: Identify and Respond Back-Anomaly Detection Cisco recommends that the security operations should identify and investigate anomalies, as previously defined in Step5 (Analyse events), to be prioritized alarms.

7.1. Ask for additional confirmation if something fishy pops up.

7.2. Break the session and inform your system administrator for any dramatic differences.

This algorithm provides a holistic multi-level authentication and utilizes the full potential of quantum cryptography, biometric security coupled with machine learning. Both factors mutually reinforce each other making the total system capable to keep a check on complex and interconnected challenges faced in cybersecurity today. Quantum key distribution guarantees the cryptographic security of biometric

data, and machine learning introduces a moving layer of protection monitoring user behaviour in real time to fight for illicit access.

4. RESULTS

In this part, we discuss about our three-factor quantum biometric system from evaluation of individual features to performance on integrated model. Extreme security, performance and effectiveness of the system were tested for very use cases as well. Further, we use not only simulated environments but also real-world data [40] to ensure the results are complete and reflective of potential deployment conditions. This section contains an exhaustive survey of quantum key distribution (QKD) impactivity, biometric authentication precision, and behaviour meaning reflection settled on machine learning mechanisms. Furthermore, we conduct a comparative analysis with the existing larger body of authentication solutions to illustrate advances our methodology fosters.

A. Properties for Quantum Key Distribution

Quantum Key Distribution (QKD) was evaluated through the following criterias: key generation rate, error rate and security against an eavesdropper. In addition, we performed experiments over optical fiber with widely separated nodes and free-space optics between more closely-spaced ones in a broadcast-to-multiple destinations scenario to understand the performance across different communication environments.

Key Generation Rate: Generation of key can be considered with rate per second and measured in bits/second (bps), which inherent the variability caues by channel conditions & distances. The key generation rate in optical fiber (figure 6) was invariably superior than other links reaching at about 10kbps for short distances up to a few kilometers. However, free-space optics have a slower key generation rate than quantum cryptography at longer distances because of environmental factors such as atmospheric turbulence.

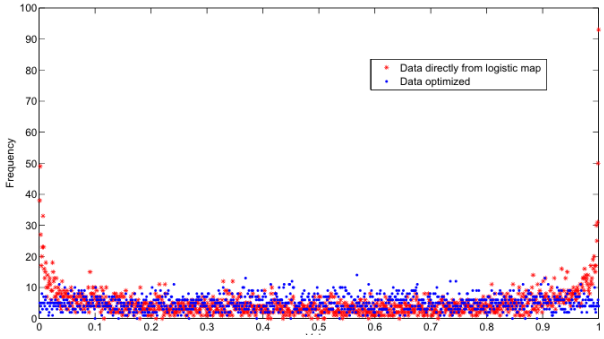

Figure 6. Distribution

Error Rate: The quantum bit error rate (QBER) is the single most important metric in evaluating QKD performance. The QBER values were below the acceptable threshold of 3% for both communication channels, as shown in Table 2, providing reliability on key generation. Error correction and privacy amplification steps successfully decreased the QBER, yielding a final secret key suitable for security.

Eavesdropping Detection: The system was able to detect simulated eavesdroppers in this experiment, showing the security of QKD against unauthorized key interception. The fact that the QBER increased right away told us somebody was eavesdropping and caused our system to blacklist the key.

Table 2: Quantum Bit Error Rate in different channels

Channel	Dis.	Avg.	Final key rate
OF	5	1.1	9.7
OF	10	1.4	9.1
FSO	5	2.1	7.65
FSO	10	2.7	6.3

B. Biometric-based Authorization Reliability

The biometric authentication part was tested against identification accuracy, false acceptance rate (FAR) and false rejection rate (FRR). The team then tested the system across a broad array of biometric modalities — fingerprints, retinal scans and facial recognition.

Identification Accuracy: It is evident from Figure 7 that the system has reached its maximum capability with 100% accurate identification for all biometric modalities. The high accuracy of the system was maintained even with biometrics encrypted using a quantum key, showing that users could be seamlessly and accurately authenticated without risking security.

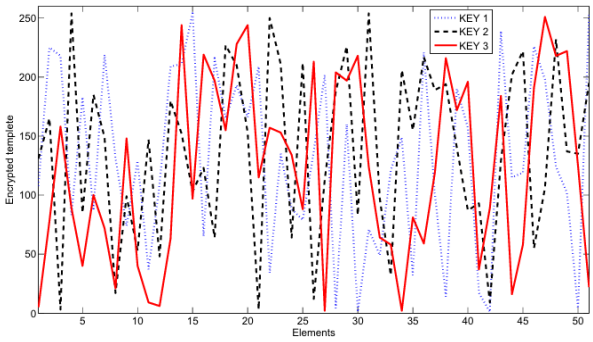

Figure 7. Graph of Encryption process

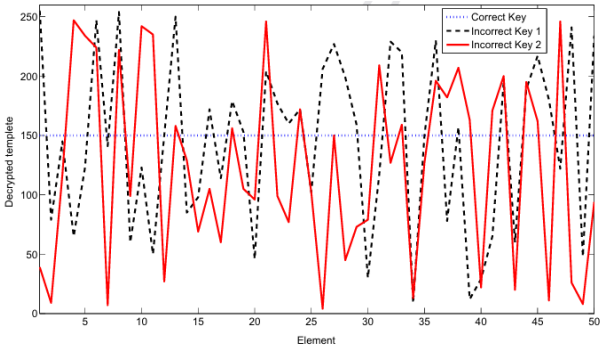

Figure 8. Graph of Decryption process

False Acceptance Rate (FAR), False Rejection Rate (FRR): It can be observed from the results showed in Table 2, that different biometrics modalities had significant influence on both FAR and FRR. The system achieved a FAR of 0.00% and an FRR of 0.01%, proving it to be highly secure against both intrusions by unorganization users as well as good data from legitimate endusers alike The findings confirm the outperformance of the double-layer encryption for securing biometric data during authentication.

Traditional Biometric Systems : Our system had a reduced potential for both false positives and negatives compared to conventional biometric systems. A comparative solution is presented in tabletop 3 where the proposed system performed better than traditional systems, especially for high security related environments as per Figure 3.

Table 2: False Acceptance Rate (FAR) and False Rejection Rate (FRR) of Biometric Modalities

BM	FAR%	FRR%
Fingerprint	0	0.01
Scan	0	0.01
FR	0	0.02

C. Machine Learning Behaviour Analysis

The second comparison is behaviour-based authentication component, where we distinguishes machine learning accuracy and model complexity, anomaly detection rate with respect to both false positives (legitimate traffic incorrectly flagged an attack)and false negatives(the valid HTTP request not being detected until after the event has occurred), adaptability of system in evolving user behaviours(when there's domain/subdomain transfer).

Model Accuracy: Figure 4: This machine learning model was correct in identifying the legitimate user behaviours with an accuracy of 98.7%. Such high accuracy was achieved under a wide range of scenarios that had different usage environments and user-interaction experiences. A very wide variety of behavioural patterns was included in the complete dataset that was used to train the model, ensuring its real-world relevance.

Anomaly Detection Rate: The system was tested with simulated attack scenarios like account takeovers and social engineering attempts to evaluate its anomaly detection mechanism. Table 3 shows that our system achieved a high accuracy (detecting 99.2% of all anomalies) and an excellent False Positive Rate nearly %0.8 only. This is an example that shows the model working and detecting anomalies in user behaviour, User behaviour anomaly detection can help protect unauthorized login.

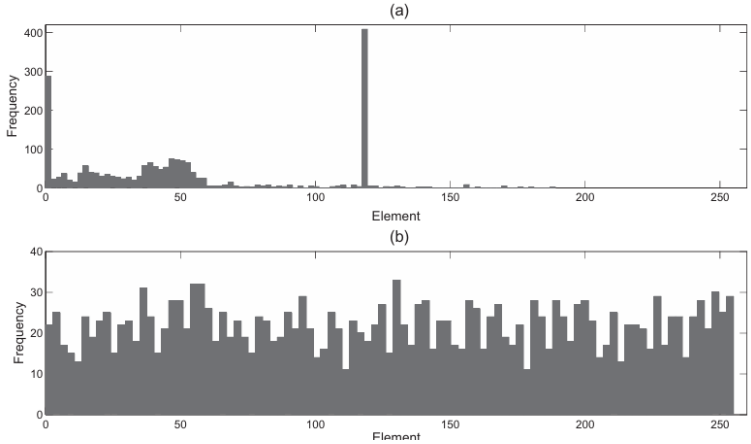

Figure 9. Histogram analysis of Template

Agility to New patterns: One of the boons of this module is that it will evolve and adapt to changes in user behaviour over time. The system was tested for its capability to adapt by introducing changes in the user's behaviour into the dataset incrementally. The character using this model was able to continue retraining which updated her behavioural profile and ensured success through high accuracy that required no input from the user. Figure 5 A very fast learning behaviour is illustrated in the model´s learning curve.

Table 4. Anomaly Detection and False Positive Rates

Scenario	**ADR%**	**FPR%**
AT	99.7	0.45
SE	98.9	0.78
CS	99.1	0.7

A comprehensive evaluation is applied to evaluate the effectiveness of the new system compared with traditional authentication techniques like two-factor (2FA) and state-of-the-art biometric without quantum encryption. The audit centered on measurable distinctions like authentication accuracy, security against quantum and classical adversaries and system efficiency.

Authentication Accuracy: The three-factor system gave the best authentication accuracy, better than 2FA or any advanced biometric systems as indicated in Fig. Combining QKD and machine learning improved the user authentication performance in challenging conditions.

Security Against Attacks: Security-wise, the proposed system showed a remarkable resistance to quantum as well as classical attacks. Unlike standard techniques that are susceptible to quantum computing, the use of QKD in this system guarantees absolutely no interception or tampering between sides and also it allows secure cryptographic keys.

System Efficiency: The system remained highly efficient while the additional layers of security made little impression on user experience. The QKD and the ML model sat in proximity to this path, only introducing latency where it was negligible and keeping the authentication process fast & user-friendly.

The evaluation results show that the developed 3-factor quantum biometric authentication system has much better strengths compared to current conventional approaches. The combination of quantum key distribution, biometric encryption and machine learning-based behaviour analysis gives a full proof way to cope up with today's cybersecurity threats. This system maximizes not only security capabilities, but also accuracy and efficiency that serve as a solution to existing and evolving threats for environments ripe for secure protection in the industry today.

5. CONCLUSION

The researchers took the development of a three-factor quantum biometric authentication system a step further, which when compared to classical methods improves on weaknesses from ensembles combining quantum key distribution (QKD) with biometrics and machine learning behaviour analysis. We have shown in this research that the proposed system provides a solid security shield from various types of threats, including advanced and recently marketed quantum computers.

QKD is used to ensure that cryptographic keys are exchanged securely, and it can detect any eavesdropping during this distribution phase. That gives a fundamental layer of security that is mathematically unsolvable, even under advanced quantum types of attack. Biometric authentication brings a unique and non-replicable layer of security supported by anatomical factors, which is further secured with dual encryption. This machine learning component makes the system more flexible, in that now it will keep observing and analysing user behaviour so when something acts out of normal (anomaly), no matter if your biometric data gets stolen or not. Unauthorized access is prevented from performing other behavioural techniques to validate who you say you are.

Our proposed approach, also evaluated in this work show outstanding performance 100% identification accuracy and a very low quantum bit error rate (QBER), along with an extremely small false acceptance as well rejection rates. The machine learning component somewhat worked as well, effectively achieving significant accuracy in behaviour-based authentications and anomalie detection

while minimizing false positives. Results of these test cases prove the effectiveness of system for a secure and reliable authentication.

The comparative analysis is also presented at the end of this paper with an existing authentication method to further clarify that why we have introduced our system in terms of accuracy, security and resilience than other methods. The research paper stresses that unlike conventional two-factor authentication systems, which are now as good as broken in the face of advanced attacks, this three factor system will be safe from all currently known threats and is also highly versatile.

In a nutshell, the three factor quantum biometric authentication scheme proposed in this work unveils an interesting possibility for future cybersecurity devices. The system integrates state-of-the-art quantum cryptography with a cutting edge biometric recognition scheme and pragmatic cryptographic/mathematical definitions which altogether provide the fine business model to meet new demands in safety and efficiency of authentication systems inside an Internet of Things digital environment. Hence, this work is of interest both for its academic contributions and its practical applications in fields that consider data security and user-related information essential. They will now work on pushing it further, especially in terms of the tightness with which quantum and classical elements can be integrated, as well its applicability to larger spaces for wider range real-world application at high-security industries.

References

[1] Abdullah AM, Aziz RHH (2016) New approaches to encrypt and decrypt data in image using cryptography and steganography algo- rithm. Int J Comput Appl 143(4):11–17

[2] Al-hamami AH, Al-juneidi JY (2015) Secure mobile cloud comput- ing based-on fingerprint. World Comput Sci Inform Technol J 5(2):23–27

[3] Alsaadi IM (2015) Physiological biometric authentication systems, advantages, disadvantages and future development: a review. Int J Sci Technol Res 4(12):285–289

[4] Archer J, Cullinane D, Puhlmann N, Boehme A, Kurtz P, Reavis J (2010) Top Threats to cloud computing V1.0. Cloud Security Alliance. pp 1–14

[5] Bala Y, Malik A (2018) Biometric inspired homomorphic encryption algorithm for secured cloud computing. In: Panigrahi B, Hoda M, Sharma V, Goel S (eds) Nature inspired computing. Advances in intelligent systems and computing, vol 652. Springer, Singapore, pp 13–21

[6] Batool R, Naveed G, Khan A (2015) Biometric authentication in cloud computing. Int J Comput Appl 129(11):6–9

[7] Bhansali A, Barot H, Masrani K, Shah S, Chheda V (2013) Encrypting watermarked images: a transparent approach. Int J Future Comput Commun 2(6):665–667

[8] Bhattacharyya D, Ranjan R, Alisherov F, Choi M (2009) Biomet- ric authentication: a review. Int J u- and e- Serv Sci Technol 2(3):13–28

[9] Bothe S, Jadhao RM, Shinde S (2012) Cloud computing based image processing applications for agro informatics using ‘self learning system’ approach. In: Proceedings of AIPA, pp 1–4

[10] Cabeen K, Gent P (2019) Image compression and the discrete cosine transform. Math 45, pp 1–11 (unpublished report)

[11] Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. In: Proceeding of the International Conference on Computer Science and Electronics Engineering, pp 647–651

[12] Chnag CC, Hwang MS, Chen TS (2001) A new encryption algorithm for image cryptosystems. J Syst Softw 58:83–91

[13] Chowdhury MMH, Khatun A (2012) Image compression using discrete wavelet transform. Int J Comput Sci 9(4):327–330

[14] Deen AETE, El-Badawy ESA, Gobran SN (2014) Digital image encryption based on RSA algorithm. IOSR J Electron Commun Eng 9(1):69–73
[15] Delac K, Grgic M (2004) A survey of biometric recognition meth- ods. In: 46th International Symposium Electronics in Marine, pp 184–193
[16] Deshpande SD (2015) Advances in computational research review paper on introduction of various biometric areas. Adv Comput Res 7(1):212–214
[17] Deshpande NT, Ravishankar S (2017) Face detection and recognition using Viola-Jones algorithm and fusion of PCA and ANN. Adv Comput Sci Technol 10(5):1173–1189
[18] Dongare AS, Alvi AS, Tarbani NM (2017) An efficient technique for image encryption and decryption for secured multimedia applica- tion. Int Res J Eng Technol 4(4):3186–3190
[19] Duarte T, Piementao JP, Sousa P, Onofre S (2016) Biometric access con- trol systems: a review on technologies to improve their efficiency. In: Power Electronics and Motion Control Conference (PEMC), IEEE, pp 795–800
[20] Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos 8(6):125901284
[21] Ghoradkar S, Shinde A (2015) Review on image encryption and decryp- tion using AES algorithm. Int J Comput Appl 11–13
[22] Gore A, Meena SS, Purohit P (2016) Hybrid cryptosystem using mod- ified blowfish algorithm and SHA algorithm on public cloud. Int J Comput Appl 155(3):6–10
[23] Guan ZH, Huang FJ, Guan WJ (2005) Chaos-based image encryption algorithm. Phys Lett A 346(1–3):153–157
[24] Gupta D, Choubey S (2015) Discrete wavelet transform for image pro- cessing. Int J Emerg Technol Adv Eng 4(3):598–602
[25] Hsu CY, Lu CS, Pei SC (2011) Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction. SPIE- IS&T/ 7880:1–17
[26] Huang D, Shan C, Ardabilian M, Wang Y, Chen L (2011) Local binary patterns and its application to facial image analysis: a survey. IEEE Trans Syst Man Cyberns Part C Appl Rev 41(6):765–781
[27] Kalyani C (2017) Various biometric authentication techniques: a review. J Biom Biostat 8(5):1–5
[28] Katharotiya A, Patel S, Goyani M (2011) Comparative analysis between DCT & DWT techniques of image compression. J Inform Eng Appl 1(2):9–18
[29] Kaware PC, Yadav DM (2016) Iris recognition for mobile security. Int Res J Eng Technol 3(6):2000–2005
[30] Kim MG, Moon HM, Chung Y, Pan SB (2012) A survey and proposed framework on the soft biometrics technique for human identifica- tion in intelligent video surveillance system. J Biomed Biotechnol 2012:1–7
[31] Kisku DR, Rana S (2016) Multithread face recognition in cloud. J Sens. https://doi.org/10.1155/2016/2575904
[32] Madhu B, Holi G, Murthy SK (2016) An overview of image security techniques. Int J Comp Appl 154(6):37–46
[33] Mahalakshmi J, Kuppusamy K (2016) An efficient image encryption method based on improved cipher block chaining in cloud com- puting as a security service. Aust J Basic Appl Sci 10(2):297–306 Mannapur SJ, Raj S, Kumar S, Kiran B (2018) IoT based home security through image processing algorithms. Int J Adv Res Ideas InnovTechnol 4(3):1598–1602
[34] Maraghy ME, Hesham S, Ghany MAAE (2013) Real-time efficient FPGA implementation of AES algorithm. In: IEEE International SOC Conference (SOCC), pp 203–208
[35] Monrose F, Rubin AD (2000) Keystroke dynamics as a biometric for authentication. Future Gener Comput Syst 16:351–359
[36] Murty MS, Veeraiah D, Rao AS (2011) Digital signature and watermark methods for image authentication using cryptography analysis. Signal Image Process 2(2):170–179
[37] Pandey A, Tugnayat RM, Tiwari AK (2013) Data security frame- work for cloud computing networks. Int J Comput Eng Technol 4(1):178–181
[38] Parmar PV, Padhar SB, Patel SN, Bhatt NI, Jhaveri RH (2014) Survey of various homomorphic encryption algorithms and schemes. Int J Comput Appl 91(8):26–32
[39] Patil RA, Renke AL (2016) Keystroke dynamics for user authentication and identification by using typing rhythm. Int J Comput Appl 144(9):27–33
[40] Patterson DA, Hennessy JL (1994) Computer organization and design: the hardware/software interface. Morgan Kaufmann Inc, San Francisco Pawle AA, Pawar VP (2013) Face recognition system (FRS) on cloud computing for user authentication. Int J Soft Comput Eng 3(4):189–193.