RESEARCH ARTICLE

European Journal of Information Technologies and Computer Science
www.ej-compute.org

Authenticating Data Transfer Using RSA-Generated QR Codes

Angela Marie S. Pangan, Izrah L. Lacuesta, Romie C. Mabborang, and Flordeliza P. Ferrer

ABSTRACT

Lack of security measures for cybersecurity threat is somewhat vulnerable and can even put one's digital life at high risk of phishing attack which is so alarming nowadays. Perpetrators may even use fictitious personal information to infiltrate various institutions for their malicious acts. It is the aim of this paper to present a security measure for a safe data transfer by means of vaccination card. Vaccination information is one of the most commonly acquired pieces of data today. However, because most internet data collection processes lack encryption, personal data becomes very vulnerable to threats. As a result, the researchers presented a Centralized Covid-19 Record System, which illustrates secure data transfer via RSA-generated QR codes. A descriptive research design was employed in which a survey questionnaire together with secondary data sources and online tools i.e., RSA Express Encryption/Decryption Calculator and QR code generator were utilized as data instruments. Through a culmination of knowledge on asymmetric cryptography, RSA algorithm, QR codes, and web system development, answers to the founded research questions were unveiled. The web system's architecture comprises several components and sub-components building its digital makeup. For the system development process, the most essential structural components are the web browser, web server, and database server. Through a message encryption/decryption feature that makes use of the RSA algorithm in generating a key pair, cryptography was implemented in the system. The essential mathematical parameters comprising such features are RSA encryption algorithm, RSA decryption algorithm, and Euler phi function. As for the system development environment, several hardware and software requirements that build and support the system's end-to-end process were also specified. Upon the employment of those specifications, the system was able to offer several security features including the 15-digit account user IDs and QR code scanning for log-in, secured acquisition of public and private keys, and an admin verification process. Lastly, it was found that asymmetric cryptosystem provides a secured channel for data transfer due to the computational difficulty of factoring the large integers that constitute modulo n. Upon the strategic culmination of the study's framework, well-established system architecture, required system specifications, and security measures, the researchers were able to successfully develop VacciFied.net, a Centralized Covid-19 Record System involving authenticated data transfer process.

Keywords: Asymmetric Cryptography, Encryption, Decryption, RSA algorithm, QR codes, Web-based system.

Published Online: August 31, 2022

ISSN: 2736-5492

DOI :10.24018/ejcompute.2022.2.4.73

A. M. S. Pangan
Pamantasan ng Lungsod ng Maynila (University of the City of Manila), the Philippines.
(e-mail: amspangan2018@plm.edu.ph)

I. L. Lacuesta
Pamantasan ng Lungsod ng Maynila (University of the City of Manila), the Philippines.
(e-mail: illacuesta2018@plm.edu.ph)

R. C. Mabborang*
Pamantasan ng Lungsod ng Maynila (University of the City of Manila), the Philippines.
(e-mail: rcmabborang@plm.edu.ph

F. P. Ferrer
Pamantasan ng Lungsod ng Maynila (University of the City of Manila), the Philippines.
(e-mail: fpferrer@plm.edu.ph)

****Corresponding Author***

I. Introduction

As an essential component of everyone's daily lives, the internet has been a channel where people share most of their data, including sensitive personal information. However, existing online systems rarely include an encryption procedure over network channels. As a result, data transferred over the internet is extremely vulnerable to attacks and illegal activities, resulting in considerable loss of security and integrity.

Especially when the Covid-19 pandemic started, the world relied on technology to lessen physical contact and contain the spreading of the virus. Most of these activities, such as banking and office work, require a lot of data transfer over the internet and may need you to upload sensitive personal information. For example, to gain access to establishments and government offices, one must submit one's vaccination card and valid ID – which includes data such as name, birthday, and address.

As found by the researchers, the current vaccine card validation process prioritizes the issuance of vaccine passports/certificates to domestic and international travelers only, resulting in the lack of an effective and convenient centralized system to verify a person's vaccine history and personal information. Only around 58 percent of Filipinos have been properly vaccinated, according to the World Health Organization (2022), which means there are still millions of data to be received and evaluated. As a result, it is critical to keep improving the country's existing verification mechanisms in order to meet the growing need for security and confidentiality.

Because of their large data capacity, QR codes are recommended as one of the most effective and intuitive ways to communicate data for various purposes. However, current QR code systems use an unsecured data structure that rarely uses encryption. The user's own manual handles the majority of personal information confidentiality in an insecure manner, making data highly vulnerable to breaches and security hazards. Hence, for secured and smart transactions over networks, the researchers incorporated the concept of QR codes and asymmetric cryptography in the study.

VacciFied.net, the researchers' proposed data transfer system, illustrates centralizing Covid-19 records and securing message transit between users and administrators. A localized record database was employed in the system to store personal and vaccination information for authorized users. Institutions could use the proposed method to collect and verify user vaccinations for smoother entrance to their facilities. For instance, in the university, the proposed record system may be utilized to check user verification and allow students and/or professors entry without having to provide vaccination cards or identification.

A. *Conceptual Framework*

To provide a schematic diagram that can best conceptualize the study, a flow chart system was used. Basically, all the processes implemented revolve around the Centralized Covid-19 Record System (*VacciFied.net*) that the researchers designed. It makes use of web browser and server/database as its support and control system to enable its operation.

Proper implementation of the framework will guarantee success in applying RSA cryptosystem for a secured data transfer.

B. *Statement of the Problem*

The goal of this research was to demonstrate an authorized data transfer utilizing an RSA-Generated QR code system. The following questions were addressed by this study:

1. What comprises the system architecture (framework) of the study?
2. How was cryptography implemented in the system?
3. What parameters/algorithms are involved in the processes of key generation, encryption, and decryption?
4. What are the requirement specifications of the system?
5. What security features characterize the proposed system?
6. Why is asymmetric cryptosystem a secured channel for data transfer?

II. Related Literature

A. *Authentication Mechanisms and Classification*

An important component of authentication is the need for communication between two parties. Security must be considered from confirmed authentication to the secured establishment. In many cases, these parties may communicate over different channels which may be in private or in public networks. There are also different authentication options for IoT devices. In a research from [1], they described the gaps and opportunities in current IoT authentication techniques as weak transport encryption, password limitation, faulty or complication IoT systems, broken authentication and authorization, and security flows in device software. The complexity of an authentication scheme may vary depending on the parties involved in communication, and the different methods that they use. Some of these methods may be based on particular criteria such as memorability, graphics, body specifics, QR codes, or combining different techniques [2].

According to [3], two-factor and multi-factor authentication have been increasingly common in recent years as cloud computing has become more accessible and popular. One of the most common examples of this form of authentication is Google's two-step verification, which uses a software-based process to add a second layer of security. Google Authenticator generates two-step verification tokens in addition to the account password, which are utilized during the log-in procedure for a more secure entry process. Another type of two-step authentication is the use of hardware tokens like an RSA SecureID, which creates a fresh six-digit verification code at set intervals of thirty to sixty seconds [4]. Authy, Duo Security, RSA SecureID Access, Azure Multi-Factor Authentication, LastPass, Ping Identity, AuthPoint Multi-Factor Authentication, and others are some of the software counterparts that employ this type of authentication process. Once each is configured, their usage is straightforward.

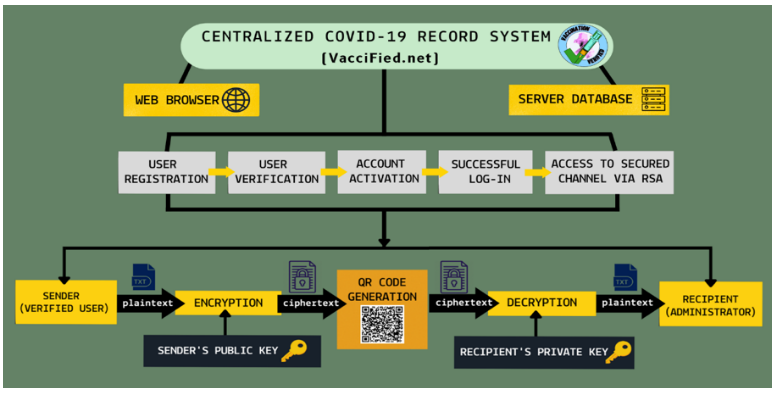

Fig. 1. VacciFied.net Conceptual Framework

B. Security Threats and Countermeasures

According to [5], the threat models in the two-factor authentication scheme for mobile money are classified into five categories: attacks on privacy, attacks on authentication, attacks on confidentiality, attacks on integrity, and attacks on availability. Personal identification, both numerical and biometric, has been identified as a countermeasure. PIN, OTP, and QR code mechanisms are examples of number-based countermeasures, whereas biometric countermeasures can be physiological, such as fingerprint, face, and retina recognition, or behavioral, such as voice recognition. The use of cryptographic functions is another countermeasure.

Cryptographic algorithms and modes of operation are used to define cryptographic functions. They aid in the achievement of the security goals of confidentiality, authenticity, and integrity in the two-factor authentication scheme for mobile money. Asymmetric encryption functions, symmetric encryption functions, and hash functions are the most commonly used cryptographic functions in mobile money's two-factor authentication scheme. Elliptic curve cryptography (ECC) and the Rivest-Shamir-Adleman (RSA) encryption algorithm are two examples of asymmetric encryption functions used in the two-factor authentication scheme for mobile money [6]. Furthermore, the scheme's use of an encrypted QR code with RSA ensured the user's legitimacy, information confidentiality, integrity, and accuracy in mobile payment. This is accomplished by implementing a mutual authentication method via a Public Key Infrastructure system, which secures key distribution, verifies the sender and recipient as legitimate users, and ensures the confidentiality of data information [7]. This encryption system employs the RSA algorithm, which is widely regarded as the most secure asymmetric encryption system. Along with this, the integration of QR codes as a mode of payment ensures the integrity, legibility, and confidentiality of the information, laying a solid foundation for system security.

A Memory Efficient Multi-Key (MEMK) generation strategy for secure transmission of sensitive data through cloud and IoT devices is the solution to lightweight protocols' cryptosystem security problems. The suggested approach is beneficial since it minimizes the amount of processing resources required for the RSA algorithm. Thus, the solution can be used in low storage or processing power device [8]. IoT usually has small memory and processing power. That is why only lightweight cryptosystems are used in a platform which attracts attackers and invite threats because these solutions are not suited well for other existing cryptosystems. When such cryptosystems are deployed in real-time computers, vulnerabilities arise; these vulnerabilities are behavior-based (e.g., calculations, time consumption, and battery usage) and might reveal the attacker insights about the system's underlying functionality. Reference [9] developed a MEMK generation strategy to assist secure data transfer between IoT devices and the cloud in their research. The RSA encryption technique, which is an asymmetric cryptosystem, was employed in the suggested system. However, because IoT devices have limitations, there is no private key in this approach. On the other hand, because of this deficiency, the inverse computation is unnecessary.

C. Self-Authenticating Identifiers

Asymmetric cryptography, often known as public key cryptography (PKC), is an encryption method that uses two mathematically connected public and private keys. PKC is distinguished from the competition by the fact that each key serves a unique purpose, with one key used to encrypt and the other to decrypt. PKC is typically used to verify digital signatures by encrypting the digital hash of a binary message, which is then decrypted by the recipient using the public key. If they match, the recipient can be confident that the sender has the private key and is the message's original sender, verifying the sender's identity. The recipient must have access to the public key in order to do this verification. CAs were formed as a result of the digital signature authentication procedure, and they produce certificates that link an identity to the public key of a PKC pair. Another significant advantage of PKC is its secrecy. A public key, for example, can be used to encrypt a message sent to the same public key's owner. The owner can only decrypt the communication if he or she has the private key, ensuring confidentiality. The public key that will accompany the certificate to the receiver is chosen by the sender. In this approach, a third party validated the certificate's owner's affiliation [10]. Although CAs have shown to be valuable in the past, some have been corrupted, undermining public confidence in authorities.

These mechanics gave rise to the concept of Trust on First Use (TOFU), in which the recipient must believe that a public key is associated with a known or knowable party. For example, if a party sends a message that says, "this is my public key," the recipient is expected to use the information to verify the source by authenticating its digital signature and encrypting it to return to the sender for the sender to decrypt and return to you. Domain names, for example, use public keys as an identifier that is associated with a unique Internet Protocol (IP) address. If the IP address is found in a registry of public key identifiers, the device can be challenged with that IP address to ensure it is still associated with a private key using the challenge/response protocol described earlier. If the device was unable to demonstrate significant bona fides to the registry, this could result in a type of TOFU-plus [11], which gives the party reaching the computer at the destination IP address greater confidence that it was the intended destination.

It may be suggested to apply this to the Internet of Things (IOT) where the IOT device generates itself a public and private key pair and self-registers its public key. For instance, a hub can verify that it has reached the correct IOT device, and the IOT device's configuration into a group could include the inclusion of the hub's public key in a valid list of devices that operate on the now-configured IOT device. If both devices still have their private keys, they can check that they are connecting with the device that runs on the original setup. Though it may not be apparent, failing to validate an identification using this method does not provide much information to the user who demands verification. Physical presence, Bluetooth key pairing, or any other action that enhances confidence in the registration process, such as proximity NFC, are all required to register a device with a hub or controlled user. To increase trust in the process, QR codes and public key strings associated with a registration device must be recorded by a mobile camera or decrypted by

DOI: http://dx.doi.org/10.24018/ejcompute.2022.2.4.18

a configuring party.

D. Two-Dimensional Barcodes Security Risks and Solutions

Barcodes have taken over most marketing firms and business establishments around the world in recent years. Its primary goals are to store information and allow consumers to easily read and scan it using their devices. However, as the use of 2D barcodes grows in popularity, it has attracted the attention of cyber attackers looking to access users' private personal information or directly compromise users' smartphones and any other connecting device they own. As a result, understanding possible barcode attacks and prevention or protection techniques is both important and difficult. When there is a lack of content authentication and is easily mounted, there is a high possibility of an attack; in essence, this covers the majority of barcodes we have today.

Previous research has identified various types of 2D barcode attacks, as well as various solutions to prevent them. There are at least six possible attacks. When an attacker attempts to obtain sensitive personal information by encoding a malicious web address inside a barcode, the user is redirected to a bogus web page that appears to be legitimate. Malware propagation occurs when attackers use QR codes to redirect users to malicious sites that install malware invisibly using vulnerable applications on the user's device. Attackers may tamper with and/or counterfeit barcodes from reputable companies and advertise false product information or special offers, leading victims to purchase a different bogus product. Another attack scenario involves injecting malicious JavaScript code into trusted HTML pages and executing it in an application. Cross-site scripting occurs when a script appears and runs in the context of a trusted page accessed by the user. Finally, reader application attacks rely on requesting full access to a user's device information such as location, contacts, and photos. If the application is vulnerable, a crafted barcode can trigger it, allowing the attacker to access the user's private and sensitive data.

According to [12], while many of the available barcode security systems provide cryptographic solutions, they are insufficient because they do not always adhere to the most recent recommendations and do not provide enough detail to evaluate their effectiveness. Norton Snap QR code is an Android mobile application that identifies safe websites and blocks malicious, phishing sites as an example of a solution application. It also prevents malicious websites from redirecting automatic malware downloads and fraud. Another example is the Secure QR and Barcode Reader, which provides barcode scanning while also improving phone security by preventing permissions to access personal data, preventing sensitive user information from being leaked.

Most of these solution applications still lack critical details such as key lengths, encryption algorithms, and hash functions. The use of high-quality cryptographic techniques to protect 2D barcodes from security threats is still an open discussion. As a result, conducting research on new comprehensive solutions to barcode threats is critical, as is testing various cryptographic mechanisms and security parameters to determine the best security feasibility trade off.

E. Usable Cryptographic QR Codes

In the commercial world, QR codes are commonly used for advertising, monitoring, ticketing, and marketing. People have become so accustomed to scanning QR codes that they automatically trust the content. However, not all QR codes are genuine, and users are obliged to respect the code's confidentiality. Various threats have been identified and specified for these codes. Such attacks are successful against ordinary individuals who place their trust in fraudulent websites and are unaware of malware spread. QR codes are vulnerable to these types of assaults, in which malicious content is encoded in the barcodes to intrude on the user's privacy, obtain credentials and sensitive information, and redirect to dangerous websites. QR codes are used so frequently in these security threats that they have become the major input medium and source of these assaults.

According to [13], incorporating a digital signature to QR codes inhibits the attack scenarios mentioned above (phishing, malware spreading, and so on) only when an attacker is unable to conduct a legitimate signature. Identifying a duplicate to a legitimate signature in an open-system environment would be difficult since a Public Key Infrastructure (PKI) would be vulnerable to the "HTTPS phishing problem," where attackers with valid certificates use identical names to authentic entries. In a closed or regulated environment, however, the reader may be trained to only recognizing internal certificates and validating the signature would demonstrate the QR code content's legitimacy. There are a number of additional prominent signature systems that differ in terms of performance, size, and security. All three of these criteria have an effect on the usability of QR code scanning. Digital signatures are a common and effective approach to verify the contents of a barcode and avoid most QR code assaults, especially when used in closed contexts with trusted parties' public keys. However, this is not always the case, and it is nearly never used in this scenario because QR codes are small and are typically read with smartphones, which do not have the same scanning capabilities as desktop PCs or laptops.

F. Related Studies

1) Advances on RSA Algorithm

Cryptography, defined as "the study of codes, as well as the art of writing and solving them," has been a rapidly expanding field of study in recent decades. As a result, [14] examined the strength of the RSA cryptosystem public key in a study. Because a public key is formed by multiplying two huge prime numbers, a method for factoring such a number and the time required to factor it must be investigated. Factoring algorithms such as Trial Division, Pollard's Rho, Continued Fraction, and Quadratic Sieve were all coded using this method. It is worth noting that breaking a public key necessitates an algorithm with a high time complexity, whereas protecting message data necessitates an algorithm with a low time complexity (trial division). The study's findings revealed the threshold for decrypting huge prime numbers utilized in cryptography. As a result, Trial Division was discovered to be an unsuccessful factoring algorithm (essential for the sender), whereas Quadratic Sieve was determined to be the best when it came to time complexity (and is a beneficial principle for the receiver/outside source).

DOI: http://dx.doi.org/10.24018/ejcompute.2022.2.4.18

A proposed modification to the RSA algorithm that uses four prime numbers to combine public and private keys was also investigated [15]. Aside from making the algorithm's analysis process easier (by increasing the factoring complexity of the variable), the updated encryption technique will also improve security access and speed. In the process, the number of mathematical steps was reduced by using consecutive subtraction instead of division, and an additional two prime numbers were added to the original RSA algorithm to safeguard it from mathematical attacks. The modified RSA modulus factorization was shown to be faster in terms of factoring modulus than the MREA cryptosystem, allowing for high computational performance.

Last but not least, [16] published a study concentrating on the randomization of RSA and other primary PKCs' encryption processes, implementation of two well-known randomizations (RSA-OAEP and McEliece PKC), and discussion of extensive computational difficulties and assessment methodologies for it. Security, key size, performance, transmission size, and interoperability are the primary evaluation methodologies to consider in PKCs, according to the study. On the encryption vs decryption time performance diagrams of both RSA-OAEP and McEliece PKC, encryption size (as plaintext file) is approximately linear to encryption/decryption time. Randomization of PKCs does, without a doubt, help to secure information flow on cryptosystems logically and perfectly.

2) *System Applications of RSA Algorithm*

As the challenge on authenticating data transmission remains unsolved, [17] suggested a unique algorithm in a QR Verification System utilizing the RSA algorithm, in which the sender has two keys (public and private keys) while the user only has one key (public key). The user can just view the data and not change it in this way. The Reed-Solomon code was employed in data storage, and procedures for key creation, encryption, and decryption were thoroughly explored. QR codes for image concealment and verified data encryption-decryption were successfully generated after the RSA Algorithm was incorporated into the study.

In an additional study, [18] used the RSA Algorithm to create a QR-code-based method for securing cloud data. QR codes were generated using an asymmetric key encryption algorithm and were used in deciphering encrypted text files and storing user information. Because cloud computing entails online access, manipulation, and storage of data, a detailed system design was used to create the system's webpage, which included an upload file system based on user identification and a download page system for the decrypted file. Only text files were easily encrypted using the technique utilized in the study; thus, future work will have to include a variety of files to be encrypted, such as documents, audio, and video files.

Moreover, in order to contribute to the development of effective solutions for existing validation systems, a novel protected QR code system based on the RSA cryptosystem was investigated [19]. The technology permitted authentic data transfer using QR code verification and QR code validation, which was supposed to keep personal information private. The verification technique was created using the RSA digital signature algorithm, while the validation procedure was created using the RSA public key cryptographic algorithm. The security aspects of the system prototype improved after using the Waterfall Software Development approach for the functionalities. In general, the proposed application made RSA key generation, QR code generation, QR code decoding, QR code verification, QR code validation, QR code storage, and retrieving QR code information easier.

Furthermore, [20] created a customized encryption algorithm and authentication method to fight man-in-the-middle attacks on information transfer between devices. Many devices employed a form of the Advanced Encryption Standard (AES) in the algorithm approach. The multiplicative inverse tables, S-boxes, and inverse S-boxes necessary to build each layer in the algorithm were computed using a 128-bit key (rather than a single typical irreducible polynomial). A hybrid framework was used to manage the parties' public-private keys, while a centralized server handled the communication protocol. A better strategy to verified data interchange was implemented as a result of the findings.

Lastly, in an application to the MediaSense platform (a mobile environment) for a secured distributed context exchange between networks, a security architecture that utilizes encryption algorithms, key distribution mechanism, and a safe key storage was built [21]. Following research into several options for security and privacy, the RSA process was used to act as the primary communication node for getting the first public key, with the Java KeyStore API used to secure the system's key storage. As a result, changes were made in terms of better confidentiality, integrity, and availability to give authenticity and authorization.

3) *Analysis on QR (Quick Response) Codes*

Because of their large storage capacity and damage-resistant design, QR codes are critical in ensuring security. Reference [22] did a study with the purpose of raising awareness about the importance of QR codes. QR codes can be used for a variety of purposes, including establishing calendar events, sharing one's geo position, connecting to a WiFi network, accessing URL addresses, and more. Their unique properties that make them relevant, in addition to their wide variety of functions, are: 1) omnidirectional and quick scanning, 2) tiny size, 3) vast data store capacity, 4) many sorts of data, 5) error correction, and 6) availability for everyone. However, the requirement for a QR code scanner or a QR reader app is what prevents people from using this technology.

In addition, [23] presented broad recommendations and solutions for the security and privacy of QR code applications in a comprehensive study. They looked nearly 100 barcode reader apps to see how secure and private they were. These apps were divided into five categories based on their URL Security, Crypto-based Security, Popularity, Weakness, and Save-privacy features. Following the researchers' examination, they made recommendations for creating useable, safe, and privacy-friendly programs. They want to employ *BarSec Droid*, an Android proof of concept app, because it follows their guidelines and will most likely boost the user's security trust due to its ease of use and effectiveness in scanning barcodes.

Reference [24] used compression techniques to increase the data storage capacity of QR codes with limited storage space. Multiplexing techniques were used here, such as combining bits into code words and replacing the code word with a specific sort of character. QR codes are a source of data protection as well as an information-sharing medium because they feature a two-dimensional barcode. As a result, QR codes are useful in a variety of study fields, including watermarking, steganography, and barcode scanning.

4) Quick Response (QR) Authentication System

Reference [25] presented a QR Authentication System to keep encrypted data hiding and retrieval confidential due to the significant problem of securing the secrecy of one's personal information. The markings left by users who wish to access data will be encrypted to QR Code$_{TM}$ in their new technique, ensuring that no intruder may change the marks. In this investigation, the TTJSA method, which combines three separate cryptographic modules, was employed for encryption and decryption.

Additionally, [26] developed a Secure QR Code (SQRC) technology. Despite the fact that QR codes are beneficial for data sharing and have a large data capacity, most existing QR code systems have an unsecure data structure and encryption is rarely used. As a result, validation and verification models were used as security models in their research. QR code verification was also implemented using the RSA digital signature mechanism. Overall, the suggested SQRC system proved to be effective in terms of safe data sharing.

Another study employed the QR cryptography technique to achieve reliable and secure image steganography [27]. The LSB method was used to incorporate an encrypted message inside a cover image. The Bat method was also used to hide encrypted messages in various locations. Testing of secret messages of various sizes and several cover images, as well as the adoption of a set of standard parameters, were used to assess the method's security and integrity.

Furthermore, [28] generated QR codes for Question Paper as its desktop application for data security and authentication. Here, AES Encryption algorithm was used for encryption and scanning of the QR code for decryption. Redirection to a webpage upon the transmission and online acceptance of data was also undertaken to reduce the memory storage and make way for a larger size capacity.

5) Applications of QR Code Technology

Cyber-attacks such as phishing can be experienced since QR codes are frequently utilized as physical entrances (i.e., encoded URL addresses) to internet sources. As a result, a study proposed a digital certificate-based signature with QR code verification [29]. To provide an authentication mechanism employing public and private keys, Public Key Infrastructure (PKI) technology was implemented. The public key was published using a specially constructed scanning program (App), while the private key, along with the merchant information, was utilized to create an authenticated QR code. A decoding scanner was used to verify the proposed system.

Furthermore, in a study by [30], QR codes were utilized to create a Students Attendance System that sped up the process of taking a student's attendance without generating any delays or interruptions to lecture time. To confirm attendance, participants scanned the provided QR code with their device. The class instructor used a Server Module to encrypt the QR code, which carries special information. Measures for fraud detection using GPS locations and face photos were also taken into consideration in the proposed system to eliminate fake registrations using multi-factor authentication.

6) Local Studies

The modified SHA-1 method was used in the work by [31] to check the data integrity of certificates utilizing QR code technology. During the process, the hardware and software requirements for certificate verification using the updated SHA-1 were identified. The research design is comprised of three modules: 1) QR code generation, 2) QR code printing, and 3) QR code scanning and verification. A trial run of the program was implemented by using a mixing approach for improved diffusion in the hash value and raising the hash value generated to 192 bits for enhanced strength. In conclusion, QR codes, printed certificates, and verified certificates were successfully generated with 100% accuracy using the applied technique. For future works, researchers suggest the use of optical character recognition algorithms to supplement the inspection process and the technique’s application to degree certificate verification.

Finally, [32] investigated the modification of the RSA method from creating a different value of public key 'e'. When comparing the output value and execution speed, a novel technique in the encryption and decryption process was discovered. The modified RSA algorithm, instead of just providing a different value of cipher text, generates a somewhat faster encryption process. In terms of decryption speed, there was no significant difference between the modified RSA method and the original RSA algorithm. Overall, modifying the RSA algorithm in terms of its public key can contribute to improved cryptosystem security.

With the emergence of novel technologies that pose significant privacy risks, new information concerning the gaps and opportunities in current IoT authentication systems is constantly being researched and discovered. As a result, reliable systems that can ensure the integrity and security of one's personal data are critical. Many attempts have previously been made to develop high-level barcode security systems and solution apps (such as Norton Snap QR code and Secure QR and Barcode reader). However, essential details like key lengths, encryption algorithms, and authentication mechanisms are still lacking from these methods. As a result, researchers strive to keep up with new comprehensive solutions that require evaluating multiple cryptographic algorithms and security parameters while keeping the key considerations of integrity, legibility, and confidentiality in mind.

Upon the evaluation and randomization of different PKCs, it was established that RSA cryptosystem provides the strongest asymmetric encryption function (especially when improved and modified). As a result, QR Authentication Systems with strategic integration of the RSA algorithm remain the ideal paradigm to utilize when designing security architectures.

III. Methodology

The researchers’ main objective was to provide in-depth explanation about the incorporation of RSA cryptosystem in

DOI: http://dx.doi.org/10.24018/ejcompute.2022.2.4.18

a web-based authenticated data transfer. Answering the questions about “what” and “how”, a systematic approach in describing the variables at play was discussed in this study. Starting from depicting the processes undertaken in formulating the Centralized Covid-19 Record System, the paper provided details about the programming language, system framework, system requirements, algorithms and mathematical concepts establishing the whole study. Through this approach, better understanding and a clearer view about the field’s implication will be imparted.

To give an overview of the proposed system’s structure, the researchers purposely selected open source scripting language and database system for ease of access. Open source means having a publicly accessible source code subject to an individual’s choice of usage provided their apt compliance to the distribution terms. PHP (Hypertext Pre-processor), an open source programming language was implemented to construct the web server. As for the front-end web framework, HTML (Hypertext Markup Language), CSS (Cascading Style Sheets), and JavaScript were collectively employed. These languages acted as design tools for the presentation of visual lay-out. Lastly, for the database server, MySQL, an open source relational database management system (RDBMS) was incorporated. The structured collaboration of the specified web technologies actualized the conceptualized web-based system.

A. *Respondents/Subjects of the Study*

The researchers’ proposed system requires a database of individuals’ personal and vaccine information to test the authentication of data transfer using RSA-generated QR codes. To formulate the test database, the researchers defined their study demographics as vaccinated Filipino citizens residing within the provinces of Greater Manila.

After implementing a voluntary selection process, a total of 45 respondents were gathered. Among them, 40 were representatives from the National Capital Region (NCR), 3 were from Bulacan, and 2 came from Cavite. While majority are already Fully Vaccinated with Booster (31), many are still Fully Vaccinated (14), and are yet to be given the booster dose.

B. *Data Gathering Instruments*

As the data involved in constructing a web-based system heavily relies on a programming language’s coding scheme, online articles, tutorials, and source codes on PHP scripts were utilized as secondary data instruments. Online QR code generator and RSA Express Encryption/ Decryption Calculator were also used in embedding encrypted texts on unique QR codes for decryption.

Additionally, a survey questionnaire (using Google forms) acted as the primary tool in collecting essential data for the system database. Using Facebook Messenger, Google forms were disseminated among the researchers’ contacts who qualify in the given demographics. Also, to guarantee utmost privacy and confidentiality in handling the respondents’ individual information, consent forms were correspondingly distributed among them. The data collected were classified into two divisions namely:

A. Personal Information:

1. Name;
2. Birthday;
3. Age;
4. Sex;
5. Address;
6. Contact number.

B. Vaccine Information:

1. Vaccination status;
2. Vaccination location;
3. Vaccine brand for primary series (1st and 2nd dose);
4. Vaccine brand for booster dose (optional);
5. Proof of Vaccination (Vaccine ID/ Certification).

Upon the collective use of the specified research instruments, the researchers were able to establish their proposed vaccination record system.

C. *Data Gathering Procedure*

To give an overview of the construction of the system, the researchers have utilized an open source code for an inventory system and modified it to match the requirements of a test system which authenticates data transfer using RSA-generated QR codes. The system requires the installation of the application XAMPP, which was used as a local web server in the computer. Upon installation, XAMPP was utilized to start servers MySQL Database and Apache Web Server. The source code was then uploaded to the htdocs folder of the application, along with the database SQL file which was used to insert, retrieve, and update data in the system. The researchers have pre-generated the cipher text using an online RSA decryption and encryption tool. This tool was accessed through the cs.drexel.edu site where the researchers entered the values required in the RSA encryption algorithm such as a modulus n, an encryption key e, and a decryption key d. After which the messages in plaintext were converted into cipher texts which were encrypted using an online QR code generator. These RSA-generated QR codes were added into the database SQL file. The researchers accessed localhost/phpMyAdmin/ to create the database where the SQL file was uploaded which led the system available for access through the localhost.

After establishing the validity and reliability of the instrument, the researchers distributed Google Forms where the purpose of the study was explained to the selected respondents. The researchers made sure that each participant understood the predefined criteria and consent to the processing of their personal data.

The researchers gathered information using a survey questionnaire that included personal information such as name, gender, birthdate, address, and phone number, as well as vaccination status, location, and brand of dose(s) received. The respondents were also required to show proof of vaccination and identification. The forms were reviewed and submitted to the system to be used as a test database after the respondents completed the questions.

IV. Results and Discussions

A. *System Architecture*

To provide a schematic diagram that can illustrate the elements involved in the system architecture of the study, a flow chart system was used. The architecture of the system explains the relationship and interaction between client-end, server-end, and storage-end of the system. It depicts the

DOI: http://dx.doi.org/10.24018/ejcompute.2022.2.4.18

process of triggering the website for the user to view and interact with. This process begins when the user locates the system URL and data is sent from the server to the browser, where the browser then executes the display of the requested page. If system architecture is effectively implemented, secure data transfer through RSA cryptosystems will be properly tested.

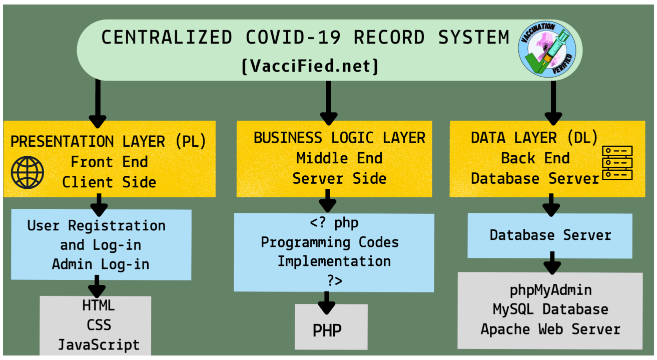

Fig. 2. System Architecture of VacciFied.net

The system architecture comprises of several components and sub-components which helps build its digital makeup. The structural components, which are most essential to the system development process are the web browser, web server, and database server. The web browser or client is the user's interface to a web system's functionality. The following can be used to create the content that is given to the client:

a. HTML/HTML5 – Hyper Text Markup Language (HTML). 'Tag' is used to generate the basic elements of websites. There are numerous tags available for displaying various types of data.

b. CSS - Cascading Style Sheet. Used to customize the websites visual elements like size, font, color, position and so on. It acts as a complement for HTML technology separating the visual aspects from the HTML tags.

c. JavaScript – A client-side script programming language that can dynamically use the HTML data. JavaScript code runs in the browser (client side). Most interactive elements of websites these days are driven using JavaScript.

d. Bootstrap - Bootstrap is a free and open-source front-end web framework for designing websites and web applications. It contains HTML and CSS based design templates for typography, forms, buttons, navigation, and other interface components, as well as optional JavaScript extensions for developing responsive, mobile-first web sites.

The web browser controls how end users interact with the program. The web system server handles business logic and data persistence and was created with PHP. Finally, the database server provides and saves data that the application requires.

B. Cryptography and System Implementation

Cryptography is a technique for encrypting data and communications so that only those with authorization can access and operate it. Additionally, it is a branch of computer science that uses mathematical ideas and a series of rule-based calculations known as algorithms to transform messages into difficult-to-decipher formats. These proposed approaches are used for cryptographic key generation, digital signing, data privacy verification, internet browsing, and confidential communications including credit card transactions and e-mail.

In today's computer-centric society, however, cryptography is most typically linked with scrambling plaintext into cipher text via encryption and then back again via decryption. The researchers utilized an asymmetric-key encryption algorithm in their study, which employs a pair of keys, one public key for encrypting communications and one private key for decrypting that information. The researchers employed the RSA encryption algorithm, which is an asymmetric-key encryption scheme to construct a message encryption and decryption function in the system, which they then deployed.

The researchers have prepared five sample messages to encrypt using the RSA generated keys. A verified user may open their account and send a secure message from their very own profile. They may choose from the five messages available: (1) Request for Admin Support, (2) Request for Profile Update, (3) Request for Profile Termination, (4) Satisfactory Experience, and (5) Unsatisfactory Experience. After choosing a message, the user should input the required public key to complete the encryption process. The message is encrypted regardless of whether the public key entered is correct or not, it is sent to the administrator along with a message status – successful and/or failed – telling when user encryption is successful, or an attempt is made by entering an invalid public key. The message is then reflected onto the administrator's database as cipher text along with the user's account ID, where the admin may choose to decrypt or delete the message. To decrypt the message, the administrator should input the required private key to complete the decryption process.

C. Parameters in RSA Algorithm

The RSA Algorithm (Rivest-Shamir-Adleman) is the foundation of a cryptosystem. The RSA algorithm has two components: (1) key pair generation, and (2) encryption and decryption algorithms.

1) Generation of RSA key pair

The researchers will demonstrate the generation of RSA key pairs that will be used in the proposed system below.

To generate an RSA key pair begins with selecting two large primes p and q. The researchers set p = 5987, and q = 4273. Next, the researchers generate RSA modulus by multiplying p and q. Thus n = p×q = 5987×4273 = 25582451. With the initial value p = 5987, q = 4273, and n = 25582451, we can select an exponent e which should not be a factor of n such that $1 < e < \phi(n)$. In other words, e and $\phi(n)$ are co-primes. The value of $\phi(n) = (p - 1) \times (q - 1)$, and so $\phi(n) = 25572192$. The researchers selected an integer which meets the criteria for an exponent e and set e = 1181. Because the public key is made of n and e, the generated public key = (25582451, 1181). Despite the fact that n is part of the public key, an attacker would have a tough time factoring a huge number and determining the two primes – p and q – needed to calculate the modulus. This is one of the most appealing aspects of employing the RSA algorithm.

Similarly, the pair of numbers (n, d) form the RSA private key. The value of d is calculated from p, q, and e. And for given n and e, there is a unique number. Private key d is the inverse modulo $\phi(n)$. This means that d is the number less than $\phi(n)$ such that when multiplied by e, it is equal to 1 modulo ϕ(n). For e = 1181, and ϕ(n) = 25572192, there is only one integer which satisfies the function e*d modulo ϕ(n) = 1. Now d = 21653, with that we obtain private key = (25582451, 21653).

2) *Encryption and decryption*

The encryption and decryption processes are quite uncomplicated and computationally simple after the key pair has been produced. In contrast to symmetric key encryption, RSA does not work directly on strings of bits. It works with modulo n numbers. As a result, the plaintext must be represented as a sequence of integers fewer than n.

The American Standard Code for Information Interchange was used to build the translation graph from plaintext to a series of numbers less than n (ASCII). Each letter was converted to its decimal equivalent using the ASCII table.

2.1) *RSA encryption*

The encryption process is a simple mathematical step as cipher text c = m^e modulo n. To calculate c, plaintext is represented first as a series of numbers less than n as demonstrated above using the ASCII Conversion chart. Using the example above, the researchers will encrypt plaintext "HI" using generated public key (25582451, 1181). In this system, each letter will be converted to cipher text. So first we encrypt plaintext H, by representing H as m = 72. By raising m = 72 to the power of e = 1181 and reduce it to modulo n = 25582451, we obtain c = 10403231. Similarly, for plaintext I and converting it to m = 73, following the appropriate calculations, we obtain c = 12190549. And so, plaintext "HI" is encrypted using public key (25582451, 1181) into c = 10403231 12190549.

2.2) *RSA decryption*

The decryption technique for RSA is likewise rather simple. Again, using the example above for cipher text c = 10403231 12190549. Each value is isolated and decrypted separately by the researchers. By raising cipher text c = 1040321 to the power of d = 21653 and reducing to modulo n = 25582451, we obtain message m = 72. Similarly, for cipher text c = 12190549, the value of message m = 73. And so, m = 72 73. Using the ASCII Conversion table, we can now convert m to plaintext and get plaintext p as "HI".

2.3) *RSA analysis*

RSA's security is dependent on the strengths of two distinct functions. The most prominent public-key cryptosystem is the RSA cryptosystem, the strength of which is predicated on the practical difficulty of factoring very large integers. The RSA encryption function is a one-way function that converts plaintext to cipher text and can only be reversed with knowledge of the private key (n, d). The complexity of deriving a private key from an RSA public key is analogous to factoring the modulus n. An attacker, unless he can factor n, cannot utilize knowledge of an RSA public key to deduce an RSA private key. It is also a one-way function; moving from p and q values to modulus n is simple but going backwards is impossible.

D. *System Requirements*

In the study, the tools in establishing *VacciFied.net* are the following:

A. Hardware requirements:

- Intel(R) Core(TM) i3-7020U CPU 2.30 GHz Processor
- 4 GB RAM
- 200 MB hard disk space
- High resolution monitor
- Webcam
- Keyboard and mouse (input devices).

B. Software requirements:

- XAMPP 7.3.0 version
- Microsoft Visual Studio Code 1.67.0 version
- Web Technologies: HTML, CSS, JavaScript, Bootstrap, Apache, MySQL
- Web browser i.e., Google Chrome
- Domain, HTTPS extension or SSL/TLS certificate (*optional)
- Web hosting provider i.e., AWARDSPACE (*optional).

It is worth noting that the *optional needs specified under software should be used **only** if you want to build online web servers. Local hosting software requirements will serve for system testing.

E. *System Security Features*

More than the incorporation of RSA Asymmetric Cryptosystem in the system's data transfer process, several features to boost its security were applied. These five features are discussed below.

1) *Account user ID for log-in*

In the registration webpage, individuals who wish to create their VacciFied.net accounts will be provided unique 15-digit Account User IDs. These Account User IDs will be difficult to crack since the possible number of 15-digit combinations we can get from numbers 0 to 9 is one quadrillion (1,000,000,000,000,000). We use the concept of permutation with repetitions to prove this since among the possible combinations of Account User ID, the minimum is 000000000000000 while the maximum is 999999999999999.

Let: $n = 10$ and $r = 15$. Using the formula for permutation with repetitions we have:

$$\boldsymbol{P(n,r)} = P(10,15) = n^r = 10^{15}$$
$$= \mathbf{1,000,000,000,000,000}$$

Hence, the probability of an attacker figuring out a registered user ID is $1/1{,}000{,}000{,}000{,}000{,}000$ or **0.0000000000000001%.**

2) *Acquisition of authorized user's unique QR code and public key*

The Authorized User's unique QR code (for log-in) and public key (for secured data transfer) will only be given upon finishing registration. Hence, only registered individuals will achieve access to the working QR code that will successfully direct them to their respective profiles (provided the Admin's Verification of their profile). Similarly, only they will know the public key for sending secured messages to Admin.

3) *Acquisition of admin's private key*

On the Admin's part, accessing the User Database Portal will only be feasible by entering the correct username and password on the Admin Log-in page. Only through successful log-in will the admin be able to acquire the private key

DOI: http://dx.doi.org/10.24018/ejcompute.2022.2.4.18

intended for decrypting the user's messages.

4) Admin verification process

Before having access to one's profile after registration, the admin needs to verify first the verification status of the newly registered individual. The admin can do so by checking first the validity of the personal and vaccine information provided by the user in the "Individual List" page. If the given information passes, admin approval will be granted, and it is only by then where the admin can change the user's verification status to "Verified" from originally being "Unverified". It is important to note that without the admin's approval, one's registration status will remain pending and inaccessible.

5) QR code scanning for log-in

It is only upon the admin's verification of the newly registered individual where the QR code will successfully work in redirecting the user to his/her profile page. The system can detect fake or unverified QR codes and immediately terminate the log-in process. Similarly, it can identify verified QR codes and successfully redirect it to the corresponding user profile page.

F. Asymmetric Cryptosystem as a Secured Channel for Data Transfer

Asymmetric Cryptosystem (also known as Public-key Cryptography) is a process that utilizes two distinct yet mathematically connected cryptographic keys (public and private) for data encryption and decryption. Its concept greatly differs to symmetric cryptosystem where only a single cryptographic key is used for both the encryption and decryption process.

Among its important properties are the following:

1. The public key is publicly used by the user/s in encrypting plaintexts to cipher texts.
2. The private key is exclusively used by the authenticated recipient in decrypting the cipher texts.
3. A cryptographic algorithm combining the encryption and decryption function is used to generate a key pair.
4. The encryption algorithm possesses a high level of complexity which makes deduction of plain text from cipher text a difficult task.
5. It provides an impenetrable form of one-way communication since it is impossible to calculate the private key from the public key.

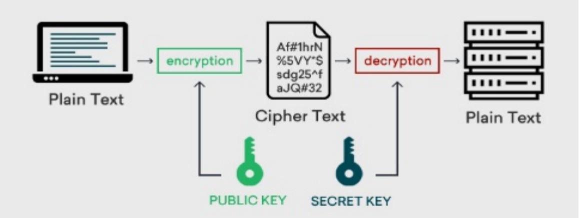

Fig. 3. Asymmetric Process: Encryption and Decryption using Different Keys.

RSA's security is derived from the computational difficulty of factoring large integers that constitute modulo n. Since only the details about public key (n, e) is made known to the public, it would be a struggle to determine the original prime numbers p and q whose product is n. More so, the time needed to successfully factor n is already beyond the capabilities of most attackers. These values of p and q are necessary because without them, generating the private key d would be impossible (remember that d is the inverse of e modulo $(p - 1)(q - 1)$).

The researchers have found that cryptography is an effective method of protecting information and communication using codes wherein only those who are authorized are able to read and process it. Thus, implementing cryptographic strategies to a web-system will ensure data privacy and authenticate data transfer. The RSA encryption algorithm, which consists of three primary processes: key generation, encryption, and decryption, is one of the most dependable forms of asymmetric cryptographies. Within this main process are the parameters of the RSA algorithm which emphasized the mathematical concepts such as the Euler phi function, involved to generate unique key pairs used to encrypt and decrypt messages.

Upon the development of the web-system (in accordance with its hardware and software requirements), and the implementation of cryptography using the RSA encryption algorithm, the system was able to offer several security features which aids in secure data transfer including 15-digit Account User IDs and log-in QR code scanning. Both of which require prior administrator verification. Through the successful testing of the proposed web system, the researchers have found that an asymmetric cryptosystem provides a secured channel for data transfer due to the computational difficulty to identify RSA generated private keys.

V. Implications to Research And Practice

The study aims to provide a framework for establishing security-related web systems. Through this research, the community will further realize knowledge on cryptography and its implementation on web systems as a preventive measure against issues of security breaches and cyber-attacks.

The findings presented will help convey valuable insights for easing data analysis of vaccine information and safeguarding messages sent over the internet. Furthermore, the study can be used in formulating institutional recommendations on managing databases which can be beneficial for both public and private sectors. Lastly, through this study, future researchers who wish to explore on authenticating data transfer using cryptography and QR codes will be guided upon.

The findings of the study could be used to design more comprehensive and enhanced web-based data authentication systems. As a result, the researchers initially advise providing a domain or an HTTPS extension to allow safe system access across many devices. Given the risks associated with online data transfer, the researchers believe that it is necessary to expand available web applications (for calculations) so that future researchers can generate larger values in key generation, encryption, and decryption, thereby making the system more secure. Additionally, expanding the type of data (to be encrypted and decrypted) from plaintext to image, audio, video, and document files is being considered as a means to improve the system's communication modality. As part of the decryption process, adding a programming function to help organize the admin's message reception in chronological order (based on the date and time the message was sent) and another function to block the receiving of "failed" encrypted messages are also suggested.

VI. Conclusion

With a well-established system architecture together with the appropriate employment of required system specifications, building a web-based system will definitely be feasible. However, considering the prevalence of the risks and challenges in protecting one's privacy online, the researchers combined the concepts of RSA Asymmetric Cryptosystem and Quick Response (QR) codes and applied it to their proposed web-based system. In the end, after a strategic culmination of the study's framework, the researchers were able to successfully develop *VacciFied.net*, a Centralized Covid-19 Record System involving authenticated data transfer process.

VII. Future Research

Future work may look into using programming languages other than PHP to offer more capabilities that would help the system improve. These features are envisioned as adding multi-factor authentication for log in (fingerprint scanning or face recognition) and installing a "attack tracker" where the administrator can instantly detect the IP address and position of illegal users attempting to access the system. For added security, consider adding a separate public key for each user. For institutions who wish to integrate the system framework in their databases, implementing a categorization process in which more than the head administrator who holds the over-all private key, administration managers would be able to access individual profiles subject to their department. Lastly, for programming experts, applying the concept of RSA digital signature technique in verifying the authenticity of information submitted is highly recommended to boost the system's integrity.

References

[1] Atwady Y, Hammoudeh M. A Survey on Authentication Techniques for the Internet of Things. Proceedings of the *International Conference on Future Networks and Distributed Systems*. 2017.

[2] Chenchev I, Aleksieva-Petrova A, Petrov M. Authentication Mechanisms and Classification: A Literature Survey. *Lecture Notes in Networks and Systems*. 2021: 1051–1070.

[3] Derhab A., Belaoued M., Guerroumi M., & Khan F. A. Two-Factor Mutual Authentication Offloading for Mobile Cloud Computing. *IEEE Access*. 2020; 8: 28956–28969.

[4] Alhothaily A, Hu C, Alrawais A, Song T, Cheng X, Chen D. A Secure and Practical Authentication Scheme Using Personal Devices. *IEEE Access*. 2017; 5: 11677–11687.

[5] Ali G, Ally Dida M, Elikana Sam A. Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. *Future Internet*. 2020; 12(10); 160.

[6] Barker E, Barker WC. Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations. *NIST Special Publication*. 2019: 800–57.

[7] Purnomo AT, Gondokaryono YS, Kim CS. Mutual authentication in securing mobile payment system using encrypted QR code based on Public Key Infrastructure. *2016 6th International Conference on System Engineering and Technology (ICSET)*. 2016.

[8] Ali RF, Muneer A, Dominic PDD, Taib SM, Ghaleb EAA. Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review. *Communications in Computer and Information Science*. 2021: 128–154.

[9] Thirumalai C, Kar H. Memory efficient multi key (MEMK) generation scheme for secure transportation of sensitive data over cloud and IoT devices. *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*. 2017.

[10] Cerf VG. Self-authenticating identifiers. *Communications of the ACM*, 2018; 61(12): 5.

[11] Farrell, S, Wenning R, Bos B. *STRINT Workshop - report/papers*. W3.Org. [Internet] 2015. [cited 2022 May 5] Available from: https://www.w3.org/2014/strint/draft-iab-strint-report.html

[12] Wahsheh HAM. Secure and Usable QR Codes. Università Ca'Foscari Venezia [Internet] 2019. Available from : http://dspace.unive.it/bitstream/handle/10579/15022/956262-1208160.pdf?sequence=2.

[13] Focardi R, Luccio FL, Wahsheh HAM. Usable cryptographic QR codes. *2018 IEEE International Conference on Industrial Technology (ICIT)*. 2018.

[14] Robinson CP. The Key to Cryptography: The RSA Algorithm. *BSU Honors Program Theses and Projects.* [Internet] 2018. Available from: https://vc.bridgew.edu/honors_proj/268

[15] Nivetha A, Preethy Mary S, Santosh Kumar J. Modified RSA encryption algorithm using four keys. *International Journal of Engineering Research & Technology (IJERT)*. 2015; 3(7): 1-5.

[16] Goyal K. Randomization of RSA and other main public-key cryptosystems. MSc Thesis. Masaryk University. 2018.

[17] Naresh K, Pillai PN. QR verification system using RSA algorithm. *International Journal of Innovation and Scientific Research*. 2014; 10(2): 433-437.

[18] Rawat V, Nath KDD, Shukla DN. QR code based cloud data protection using RSA algorithm. *International Journal of Creative Research Thoughts (IJCRT).* 2018; 6(2): 561-570.

[19] Ahamed S. Development of a secure QR code system for hiding personal confidential information. MSc Thesis. Bangladesh University of Engineering and Technology. 2018.

[20] Daddala B. Design and implementation of a customized encryption algorithm for authentication and secure communication between devices. MSc Thesis. University of Toledo. 2017.

[21] Kafle S. Securing Distributed Context Exchange Networks in Mobile Environments MSc Thesis. Mid Sweden University. 2013.

[22] Jathar C, Gurav S, Jamdaade K. A review on QR code analysis. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*. 2019; 8(7): 1-6.

[23] Wahsheh HAM, Luccio FL. Security and privacy of QR code applications: A comprehensive study, general guidelines and solutions. *Information*. 2020; 11(4): 217.

[24] Umaria MM, Jethava G. Enhancing the data storage capacity in QR code using compression algorithm and achieving security and further data storage capacity improvement using multiplexing. *2015 International Conference on Computational Intelligence and Communication Networks (CICN).* 2015.

[25] Dey S, Nath A. Confidential encrypted data hiding and retrieval using QR authentication system *2013 International Conference on Communication Systems and Network Technologies, Kolkata, India*. 2013.

[26] Ahamed S, Mustafa HA. A secure QR code system for sharing personal confidential information *International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2)*. 2019.

[27] Abed HN. Robust and secured image steganography using LSB and encryption with QR code. *Journal of AL-Qadisiyah for Computer Science and Mathematics*. 20179; (2): 1-9.

[28] Mittra P, Rakesh N. A desktop application of QR code for data security and authentication. *2016 International Conference on Inventive Computation Technologies (ICICT).* 2016.

[29] Zhang J, Liu S, Pan J-S, Ji X. Digital certificate based security payment for QR code applications. *Advances in Intelligent Systems and Computing.* 2017.

[30] Masalha F, Hirzallah N. A students attendance system using QR code. *International Journal of Advanced Computer Science and Applications*. 2014; 5(3): 1-5.

[31] Quilala R, Sison AM, Medina R. QR code integrity verification based on modified SHA-1 algorithm. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*. 2018; 6(4): 385-392.

[32] Intila CA, Gerardo BD, Medina RP. Modified key generation in RSA algorithm. *International Journal of Recent Technology and Engineering (IJRTE)*. 2019; 8(2): 1-5.

[33] Al Busafi S, Kumar B. Review and Analysis of Cryptography Techniques. 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART). 2020.

[34] Barbay J. Review of understanding and applying cryptography and data security by Adam J. Elbirt. *ACM SIGACT News*. 2012; 43(1): 18–21.

[35] Blog F. Descriptive Research Designs: Types, Examples & Methods. *Formplus*. 2020.

[36] Brush K, Rosencrance L, Cobb M. Asymmetric cryptography (public key cryptography). SearchSecurity. [Internet] 2021 [cited 2022 June 13] Available from: https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography

[37] ClickSSL. Symmetric vs Asymmetric Encryption – Know the Difference. ClickSSL Blog - Information about SSL Certificates & Infosec. [Internet] 2022 Available from: https://www.clickssl.net/blog/symmetric-encryption-vs-asymmetric-encryption

[38] codeSTACKr. Visual Studio Code 2022 | Web Dev Setup | Top Extensions, Themes, Settings, Tips & Tricks [Video]. YouTube. [Internet] 2021 Available from: https://www.youtube.com/watch?v=fJEbVCrEMSE

[39] Combinations and Permutations. Mathsisfun.com. [Internet] 2017 Available from: https://www.mathsisfun.com/combinatorics/combinations-permutations.html

[40] Czereszko G. Decrypting the future: a mathematical review of error-correcting codes and cryptography. Ball State University Libraries. [Internet] 2018 Available from: https://cardinalscholar.bsu.edu/handle/123456789/201420

[41] Daniel B. Symmetric vs. Asymmetric Encryption: What's the Difference? Trenton Systems, Inc. [Internet] 2021 Available from: https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption

[42] Development Environment: A Definitive Guide. Indeed Career Guide. [Internet] 2021 Available from: https://www.indeed.com/career-advice/career-development/development-environmen

[43] Development Environment. (n.d.). SUSE Defines. [Internet] Available from: https://www.suse.com/suse-defines/definition/development-environment/

[44] Hoffstein J, Pipher J, Silverman JH. An Introduction to Mathematical Cryptography. Springer Publishing. 2014.

[45] Isaiah A. How to add HTTPS to your website for free in 10 minutes, and why you need to do this now more than…. FreeCodeCamp.org. [Internet] 2018 Available from: https://www.freecodecamp.org/news/free-https-c051ca570324/

[46] Wright J. (2013, January 15). Learn PHP in 15 minutes [Video]. YouTube. https://www.youtube.com/watch?v=ZdP0KM49IVk

[47] Lake, J. What is RSA encryption and how does it work? Comparitech. [Internet] 2021 [cited 2022 June 13] Available from: from https://www.comparitech.com/blog/information-security/rsa-encryption/

[48] Loshin P. plaintext. SearchSecurity. [Internet] 2021 [cited 2022 June 13] Available from: https://www.techtarget.com/searchsecurity/definition/plaintext#:%7E:text=In%20cryptography%2C%20plaintext%20is%20usually,algorithms%20is%20not%20always%20plaintext.

[49] Marget A. Development and Test Environments: Understanding the Different Types of Environments. Unitrends. [Internet] 2021 Available from: https://www.unitrends.com/blog/development-test-environments

[50] Maxey M. A Modern Day Application of Euler's Theorem: The RSA Cryptosystem. [Internet] 2021 Available from: https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/maxey.pdf

[51] Mitali VK, Sharma A. A survey on various cryptography techniques. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*. 2014; 3(4): 307–312.

[52] Montero C. Centralized Covid Vaccination Records System in PHP Free Source Code|Free Source Code Projects and Tutorials. Sourcecodester. [Internet] 2021 Available from: https://www.sourcecodester.com/php/14997/centralized-covid-vaccination-records-system-php-free-source-code.html

[53] Open Source Initiative. The Open Source Definition | Open Source Initiative. Opensource.org. [Internet] 2007 Available from: https://opensource.org/osd

[54] Otto, M. Bootstrap. Getbootstrap.com. [Internet] 2000 Available from: https://getbootstrap.com/

[55] Quick Programming. Simple signup and login system with PHP and Mysql database|Full Tutorial|How to & source code [Video]. YouTube. [Internet] 2020 Available from: https://www.youtube.com/watch?v=WYufSGgaCZ8

[56] Rastogi A. PHP a Scripting Language | General-purpose programming language. NewGenApps - DeepTech,FinTech,Blockchain, Cloud, Mobile, Analytics. [Internet] 2020 Available from: https://www.newgenapps.com/technology/php/

[57] Ricart JR. A Beginners' Guide to Domain Names. Wix Blog. [Internet] 2021 Available from: https://www.wix.com/blog/2021/03/what-is-a-domain/

[58] Security, S. What is Asymmetric Encryption? Read Symmetric vs. Asymmetric Encryption Diversity. Savvy Security. [Internet] 2021 Available from: https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/#:%7E:text=Asymmetric%20Encryption %20uses%20two%20distinct,recipient%20can%20decrypt%20the%20message

[59] SourceCodester. Centralized Covid Vaccination Records System in PHP DEMO [Video]. YouTube. [Internet] 2021 Available from: https://www.youtube.com/watch?v=Mgj-zITzzcA

[60] Source Code PH. QR Code Based Centralized Covid Vaccination Records System in PHP and MySql [Internet] 2022 Available from: YouTube. https://www.youtube.com/watch?v=tyT_ZHFfaDY&t=10s

[61] The Economic Times. (n.d.). What is Ciphertext? Definition of Ciphertext, Ciphertext Meaning. [Internet] Available from: https://economictimes.indiatimes.com/definition/ciphertext

[62] Warrayat, A. Cryptography and RSA. Uga.edu. [Internet] 2012 Available from: http://jwilson.coe.uga.edu/EMAT6680Fa2012/Warrayat/EMAT%206690/Essay2/Essay2.html

[63] What is Asymmetric Encryption? Understand with Simple Examples. Savvy Security. [Internet] 2021 Available from: https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/

[64] What is Web-Based Systems. (n.d.). IGI Global. [Internet] Available from: https://www.igi-global.com/dictionary/web-based-systems/32428

[65] Why RSA Encryption is secure - RSA Encryption. (n.d.). Sites.google.com. [Internet] Available from: https://sites.google.com/site/danzcosmos/why-rsa-encryption-is-secure

A. Marie S. Pangan was born on May 16, 2000, in Pasay City, Philippines. She graduated Bachelor of Science in Mathematics as magna cum laude from the PAMANTASAN NG LUNGSOD NG MAYNILA. She served as the Public Relations Officer (A.Y. 2019-2020) and Auditor (A.Y. 2020-2021) of the PLM Mathematical Society. She was a JLSS scholar under R.A. 7687 of the Department of Science and Technology (DOST) and a PLMSFI scholar. She finished Junior High School and Senior High School at Immaculate Conception Academy of Manila where she served as the Editor-in-Chief of L'Etincelle, the school news publication (A.Y. 2015- 2016), and President of Math Club (A.Y. 2016-2017, 2017-2018). She graduated therein with High Honors and bagged Gerry Roxas Leadership Award, Mercury Drug Award for Excellence in both Science and Mathematics, and Outstanding Performance in Specific Discipline/s (Arts, Communication Arts, Science, Mathematics, and Social Sciences), etc. respectively.

I. L. Lacuesta was born and raised in Quezon City, Philippines. She graduated cum laude with a degree of Mathematics from the Pamantasan ng Lungsod ng Maynila, where she served as Secretary of the PLM Mathematical Society for three consecutive years (2018-2022). She graduated Junior and Senior High School with Honors from Escuela de Sophia of Caloocan Inc. She was chosen as school's representative during the 2017 ISAAL Science Olympiad and 2018 NPSAC Math Competition, where she emerged as Silver and Bronze medalists, respectively.

R. C. Mabborang is the chair of the Mathematics department at Pamantasan ng Lungsod ng Maynila. He has been teaching Algebra, Analysis, Discrete Mathematics, Differential Equations, Operations Research, Quantitative Methods in the undergraduate programs and Statistics in the Graduate programs for a number of years now. He graduated with the degrees of Bachelor of Science in Civil Engineering, Master of Science in Mathematics, and completed the required number of units to earn the degree of Doctor of Philosophy in Mathematics. His research interests focus on Algebra, Analysis, Combinatorics, Cryptography, Data Mining, Machine Learning, and Mathematical Modelling. He is also a Licensed Professional Teacher.

F. P. Ferrer holds a professor rank in the Pamantasan ng Lungsod ng Maynila (also known as the University of the City of Manila) where she has also handled administrative positions. A recipient of Highest Academic Distinction award when she earned the degree Doctor of Philosophy in Mathematics Education. She authored books in her field experienced from over thirty years of teaching. Her expertise is reflected in the research articles she has published in various International and Local journals over the years.