International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Illustrative Review Cryptographic Algorithms for Scada Application in Networking Ntru for Security

[1]Dr. Nitin Sudhakar Patil, [2]Dr. Shailaja Sanjay Mohite, [3]Dr. Ravindra Sadashivrao Apare, [4]Dr. Rajesh Bhatt, [5]Akanksha Kapruwan, [6]Manish Saraswat, [7]Akhil Sankhyan, [8]Dr. Anurag Shrivastava

Submitted: 04/02/2024 **Revised**: 12/03/2024 **Accepted**: 18/03/2024

Abstract: The computational applications and network protection capabilities of mobile and wireless networks have grown exponentially. Cyberattacks and other unlawful activity on commercial and personal networks have increased in recent years. Firewalls and security code fail to secure computer networks. Personal gadget users, company employees, and military personnel realise network defence is crucial. SCADA systems are commonly utilised in Critical Infrastructure Systems to autonomously monitor and control industrial activities. Security concerns are more likely in SCADA design due to its reliance on computers, networks, applications, and programmable controllers. The huge demand for computers among corporations and other organisations has led to the creation of several networks. Computer network attacks have increased in recent years. Cryptographic solutions of these requirements have performance issues in SCADA systems. NTRU, a faster and lighter public key technique for end-to-end security, is used in this research to improve SCADA security requirements.

Keywords: *Cryptographic Algorithms, SCADA, NTRU, Security, Cryptography Networking Applications.*

1. Introduction

The term "cryptology" originates from the phrase "Krypto's logos," which translates to "hidden, secret." Cryptography protects sender-receiver interactions by ensuring that the message being sent to the recipient cannot be overheard or altered in any other way by a third party. According to the data, it seems that folks live in the areas shown in Figure 1. It's possible that Machine will arrive at the conclusion that the text is encoded after it figures out that the heat is generated by ventilation, radiation, radiation, and conduction. Encryption and decryption, respectively, are the two major categories of symmetric encryption and decryption procedures. Asymmetric keys are the third primary category of symmetric encryption and decryption techniques. It is feasible to encrypt email messages by using this approach, which makes use of symmetric algorithms and paper. Due to the need of maintaining the secrecy of both the rules and the keys, the symmetric key cryptosystem is incapable of providing users with a privacy guarantee. This is because it is necessary to guard the regulations as well as the keys to the vault. When symmetrical encryption is used, the data being protected may be decrypted via the use of either a single key scheme or a pair of keys. Block-and-bit cyphers make it possible for the size of a single bit to change at a specific position in a stream. This gives the cypher more flexibility. The notion of the RC4 stream cypher, which is being explored in this article, was responsible for the creation of a cypher in the year 1987. Secure Socket Layer (SSL) and Wi-Fi Protected Access (WPA) made it possible for secure communication to take place, which was beneficial and useful for the protection of wireless internet connections. SSL is an abbreviation that stands for secure socket layer. It is also possible that it was selected rather than Wired Equivalent Privacy (WEP), a potentially harmful technology that enabled quicker, more convenient, and easier forms of communication. This is a possibility. A wide variety of ground-breaking ideas, frameworks, protocols, and strategies are now being developed to strengthen the protection of e-expanded networks. Access to a user's main email account needs knowledge of a unique password, which must be entered before the account may be accessed. Anyone is welcome to join the public key infrastructure (PKI), and once they do so, they will have access to all of the common authority keys. This may be

1HOD Electrical Engineering, Sandip Institute of Technology and Research Centre, Nashik
nitinsagar71@rediffmail.com
2Assistant Professor, Department of Mechatronics, RIT Islampur, (Autonomous under Shivaji University, Kolhapur)
shailaja.mohite1@rediffmail.com
3Associate Professor, IT Department, Trinity College of Engineering and Research, SPPU Pune
ravi.apare@gmail.com
4Associate Professor, Department of Electronics Engineering, University Departments, Rajasthan Technical University, Kota
rajeshbhattrtu@gmail.com
5Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun
akankshakapruwan@geu.ac.in
6Lloyd Institute of Engineering & Technology, Greater Noida
manish.saraswat@lloydcollege.in
7Lloyd Law College, Greater Noida
akhil.sankhyan@lloydlawcollege.edu.in
8Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu
**anuragshri76@gmail.com*

accomplished by employing either their own private key database or a shared one [1].

Using public key infrastructures, which consist of key administration as well as key management, may make this a possibility. Before the sender may include the recipient's public key in an encrypted Mail session, the receivers associated with the recipient's public key must first be set up. Even if the recipient's email is encrypted, the sender may still accomplish what they set out to achieve. Increasing the capabilities of ER or using identity-based decryption are two potential solutions to this problem. IBE makes use of IP addresses, which are also known as URLs, as names or domains, while the system makes use of names or IP addresses in their more literal sense as keys. IBE utilises URLs as names or domains. It's also possible that the names were derived from the actual meaning of the IP addresses [2].

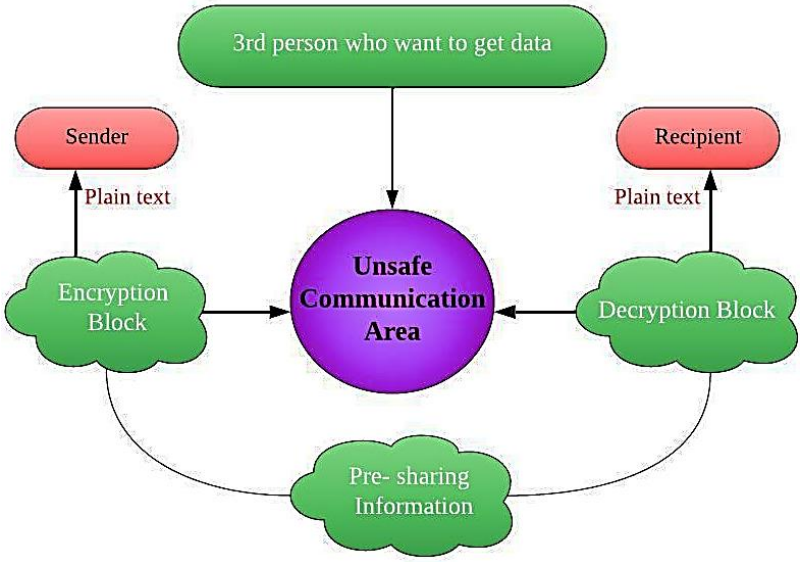

FIG 1: COMMUNICATION CHANNELS OVER THE UNSAFE AREA

According to the findings of the research, there have been many protected email security framework implementations discovered. Lu and Geva are collaborating to develop a decentralised search engine that will operate independently of the private email connection provided by GE. The use of public keys in conjunction with X.509 features make it possible for it to work. By using an email server, it establishes a connection between the emails and the properties to which they belong. As a means of providing support for important business activities, each of the systems that go into making up critical infrastructure engage in the process of exchanging real-time data from dispersed control systems across local and wide-area communication networks [3].

These systems need a method of message transmission that is efficient, cost-effective, and dependable in addition to being compliant with the appropriate communication protocol. SCADA is often used in the management systems for essential infrastructure. SCADA is a sort of control system that can remotely monitor and operate a variety of control systems, such as smart grids, chemical plants, and transportation networks, by using computers, networks, and software. This type of control system is also known as supervisory control and data acquisition (SCADA). 1960 was the year that saw the introduction of these technologies for the first time. Since that time, a number of different technological developments have contributed to the progression of SCADA. The MTU, the RTU, the Field Control Systems, the HMI, and the communication network are the primary components that make up the SCADA architecture. Multiple RTUs that are powered by site-specific microprocessors have been set up in various locations around the battlefield. They do this in order to receive sensor data remotely, which may then be used in the command centre control systems as well as the command field control systems. The primary computer in a SCADA system is referred to by its acronym, MTU. They are in charge of monitoring a number of RTUs and relaying HMI readings and data from the equipment to human operators. Additionally, they are responsible for monitoring the equipment. Human operators may potentially have a greater influence on field control systems even from a greater distance if they interpreted and sent RTU directives. It is very necessary for the functioning of the SCADA system that the control systems be connected via a communication network. Internet, leased lines, radio and microwave bands, and other types of communication spectrums are all included in these communication networks [4].

The Internet is having a huge effect on contemporary society. As a consequence of this, nobody is safe, not even those individuals who have granted the network

permission to monitor all of us and all we do. Both the data processing system and the network are safeguarded by the data security system. In most cases, management of the network itself, in addition to several layers of protection, will be included in a network security plan. When every component operates as it should, there is less variation in the overall stability of the network. Cryptography is by far the method that is used the most often in order to safeguard sensitive data. Since the vast majority of these protocols utilise unstable TCP/IP networks, users of SCADA systems have a responsibility to make the security of their systems and the mitigation of risks linked to such systems a top priority. In order to prevent unauthorised access from hackers, SCADA communications need to be both authenticated and encrypted. At the moment, the security of SCADA communications is provided by a combination of two distinct encryption methods. However, there have been complaints of performance problems with the installation, which makes it challenging to satisfy the criteria for the timely performance of the SCADA system. Validating digital signatures may now be accomplished with the use of asymmetric key techniques like RSA and ECC thanks to AGA-12, which makes this possible. Unfortunately, because to the time and processing requirements of their operation, RSA or ECC cannot be used in SCADA systems with delay constraints. This makes their use impracticable [5].

I. Review Of Literature

The capabilities of network security as well as the computer applications that may be performed over mobile and wireless networks have both increased at an exponential rate in recent years. In recent years, there has been a rise in the amount of cyberattacks and other types of illegal operations that are conducted against the computer networks of businesses and private persons. Security codes and firewalls are two techniques that are both insufficient and ineffective when it comes to the protection of computer networks. People who use their own personal technology, people who work for businesses, and those who serve in the armed forces have all come to the realisation that network security is very important. To protect the confidentiality of email communications, this piece implements an algorithmic encryption approach based on RC4 [6].

Since the introduction of the internet, one of the most significant difficulties has been protection, and in order to design new security systems, it is necessary to have an awareness of how security has evolved through time. Because of the dramatic expansion in the number of businesses and other types of organisations that need access to computers, a great number of networks have been set up. Over the course of the last several years, there has been a discernible rise in the total number of assaults launched against computer networks. In order to ensure the safety of mobile devices and wireless networks, it is necessary to design and implement brand-new frameworks that make use of certain security measures. This research has the potential to be highly helpful and is very necessary to guarantee the safety of the network. Taking into consideration the possibility that an attack may be launched against one of our networks or edge devices. In this article, we'll take a look at a variety of different approaches to network security that could be conceivable. People communicate with one another in a variety of different methods on a daily basis, some of which include the use of print media, direct mail, SMTP, social networking, search engines, bookmarking sites, and promotional email. The procedures for encrypting and decrypting data are constantly monitoring the authentication intervals to ensure that they are accurate. The duty for ensuring the safety of a network extends not only to the protection of the network as a whole but also to the protection of each individual end system. Within the scope of this essay, a variety of cryptographic and network security ideas have been dissected and discussed in length. The Supervisory Control and Data Acquisition (SCADA) system is a kind of control system that is often used in Critical Infrastructure Systems for the purpose of independently monitoring and managing industrial operations [7].

A system like this one acts as a kind of supervisory control. This article presents a discussion on the most current developments in the state of the art for a variety of cryptographic algorithms that are used in networking applications. These algorithms are intended to keep data secure. The vast majority of SCADA communication systems are susceptible to many kinds of assaults that are based on the internet. The currently applicable security requirements for SCADA communication necessitate the use of asymmetric cryptographic algorithms such as RSA or ECC. When implementing these standards' cryptographic solutions in a SCADA system that is constrained by real-time and hardware requirements, there is a possibility that certain performance concerns may arise. This thesis proposes the use of a speedier and more lightweight NTRU cryptographic algorithm for authentication and data integrity in the context of securing SCADA connections as a potential solution to the problem that has been identified. We recommend using this approach in order to solve the issue. According to the findings of an experimental research conducted with an ARMv6-based Raspberry Pi and an Intel Core CPU, NTRU cryptographic operations may be anywhere from two to thirty-five times faster than comparable RSA or ECC techniques. Because it considerably reduces the amount of processing and memory overhead, the NTRU approach is beneficial for use in SCADA systems that are constrained by the requirements of real-time operation and

the limitations of the underlying hardware. The phrase "critical infrastructure" refers to the fundamental infrastructure that is necessary for the operation of a community. Examples of critical infrastructure include water and energy supply systems, transportation and communication networks. Because the proper functioning of this infrastructure is essential to the community, it has been given the moniker "critical" infrastructure. Any action or approach that stops a real-time critical infrastructure system from running smoothly would have a harmful impact not just on the nation's security, but also on the economy and society in general. SCADA is an acronym that stands for supervisory control and data acquisition. It is a kind of control technology that is often used in Critical Infrastructure Systems. Its primary responsibility is to monitor and independently oversee all of the activities in the industrial sector [8].

Because it is dependent on computers, networks, applications, and programmable controllers, the SCADA design is more prone to security vulnerabilities and attacks than other types of systems. Common SCADA communication protocols such as IEC 60870, DNP3, IEC 61850, and Modbus do not provide any kind of security services. SCADA systems are protected from attack because more recent standards, such as IEC 62351, and AGA-12, include security measures into their design. On the other hand, there are significant performance considerations associated with the use of cryptographic solutions to these needs when SCADA systems are being used. In order to guarantee complete safety, this research makes use of NTRU, a public key algorithm that is not only more efficient but also requires less resources. As a direct result of this, it is believed that the criteria for SCADA security would work more effectively. Applications for the internet of things have been created, and they may now be used in a variety of settings, including homes, businesses, and other environments. When it comes to these applications, ensuring that data is transferred in a safe manner becomes very necessary in order to keep the system's credibility intact. The Internet of Things introduces a new paradigm in cryptography, which is known as hybrid encryption, and makes it practical to use. The performance of the symmetric key domain as well as the asymmetric key domain both see significant improvements. It makes it possible to have both high-level security and straightforward computing at the same time. In this line of study, we have recommended applying a hybrid encryption technique in order to offer information integrity, secrecy, and non-repudiation on the data transmission for the Internet of Things. In order to demonstrate the value of this method, we evaluate its efficacy in terms of how well it performs in comparison to more traditional encryption methods [9].

The use of cryptography is a major factor that contributes to the substantial enhancement of the level of data security that is maintained. Its purpose is to ensure that the contents of a communication are sent in a way that is both secret and unchanged. Network security, which is the most significant component of information security, encompasses all of the characteristics, functionalities, operational procedures, accountability, access control, and administrative and management standards of hardware and software. Cryptography is at the core of concerns over the safety of information technology since trustworthy online commerce and secure online communication are built on the pillars of privacy, secrecy, and identity. The protection of networks makes use of a broad range of cryptographic algorithms, and research is now being conducted on new cryptographic algorithms to enable more complex means of secure communication. In the present age of information technology, which includes the internet and programmes that utilise networks, the problem of data security is growing more important while also posing a number of difficult challenges. It is far more likely that anything will go wrong in a cloud setting due to the fact that the data is dispersed across such a large area [10].

The goal of data security is to restrict access to the information only to those individuals who are permitted to do so and who have a valid need to be aware of its contents. Encryption methods offer the necessary protection against attacks from data invaders by converting data from its original form into a format that cannot be read. This transformation takes place in reverse. Utilising cryptography as a strategy is one way that may be used to ensure the safety of one's data. The range of uses for cryptography has seen a considerable expansion as a direct result of recent developments in the construction of networks and instruments for communication, which have led to these breakthroughs. Cryptography is an absolute need given that it is the only technology that can both prevent monitoring and ensure that data are safe from being accessed by unauthorised parties. This article analyses the essential components of three main categories of cryptographic algorithms: hashing cryptography, symmetric cryptography (using secret keys), and asymmetric cryptography (using public keys). These categories include hashing cryptography, symmetric cryptography (using secret keys), and asymmetric cryptography (using public keys), respectively. There has been research conducted to determine whether or not the use of different cryptographic approaches can successfully protect networks and data [11].

2. Components Used in Network Security

Symmetric encryption was the only kind of encryption that saw widespread usage until the invention of public

key encryption in the late 1970s. There are a few other names for this kind of encryption, including single-key encryption and conventional encryption [12]. A wide variety of individuals and institutions, including those engaged in the military, commerce, and diplomacy, have used symmetric encryption to maintain the confidentiality of communication up to the current day. A symmetric encryption technique may be broken down into the following five components.

- ***Plaintext:*** This will be the first message or piece of information that has to be put into the algorithm. The term "plaintext," which more often goes by the name "clear text," is used in the field of cryptography to refer to material that can be read and understood without the utilisation of any additional strategies.
- ***Encryption algorithm***: Encryption is a mechanism for hiding plaintext data by changing it into a format that cannot be understood by anybody except the intended recipient. Encryption is a method that is well-known for its capacity to prevent unwanted access to sensitive data. This ability is well understood. During the encryption process, the plaintext is subjected to a number of changes and adjustments, including even being changed by a few substitutions on many occasions.
- ***Secret key:*** The use of a private key is yet another component that is necessary for the encryption process. The key contains a description of each individual change and replacement that will be made by the algorithm.
- ***Cipher text:*** When plaintext is encrypted, a form of data that cannot be deciphered, known as cypher text, is formed in its stead. This is what occurs when the meaning of the communication becomes unclear. You are going to need both the plaintext as well as the secret key in order to tackle this challenge. As a consequence of this, encryption is used to protect sensitive data from being accessed by those who are not licenced to do so. This is done even for those individuals who possess the capability of deciphering the data. When one message is encrypted using two separate keys, the outcome is not just one but two ciphertexts that are completely distinct from one another.
- ***Decryption algorithm:*** Decryption is the process of turning encrypted data back to its original plain-text format. It is often referred to as deciphering. This is, in essence, the same encryption method that is employed when reading data backwards. The ciphertext and the private key are used to produce the initial plaintext for further use (see Figure 2 for more deta

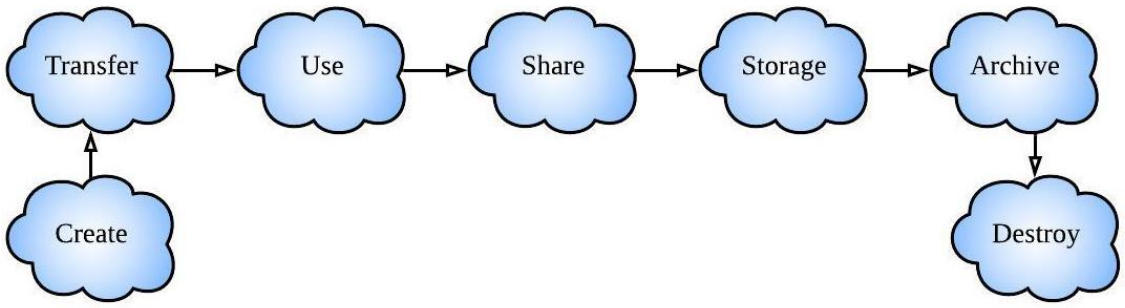

FIG 2: THE LIFE CYCLE OF DATA.

It is a generally accepted fact that the definitions of encryption and decryption as they stand now are combinations of three distinct categories of algorithms. There are three distinct categories of encryption methods, which are as follows: (i) algorithms with symmetric keys, in which the sender encrypts data using a private key and the receiver decrypts it using a public key; (ii) algorithms with asymmetric keys, in which the sender encrypts data using a public key and the receiver decrypts it using a public key; and (iii) hashing. In asymmetric key algorithms (i), the sender encrypts the data using a public key, and the receiver decrypts the data using a private key. When employing this method, the sender will never have knowledge of the private key that the receiver uses. It's possible that using hashing algorithms may assist secure the confidentiality of data. Cryptography has a wide variety of applications, one of which is user authentication. This is in addition to its primary objective, which is to prevent the theft of data and manipulation of data. Utilising cryptographic methods is necessary in order to safeguard the confidentiality of data users. Because of the high degree of complexity of the technique, there is a lower chance of successfully decrypting the cypher text and getting access to the plaintext. This is due to the increased difficulty of breaking into the market.

3. Research Methodology

In order to assure the safety of SCADA communication, the protocols for SCADA need to incorporate components such as end-to-end authentication, data integrity, non-repudiation, and secrecy. The use of cryptography is the foundation for all of these different kinds of security measures. The National Institute of Standards and Technology (NIST), the American Gas Association, and a few other organisations are currently working on defining

cryptographic standards for the purpose of securing SCADA communication. IEC 62351 is recommended for use as one of the standards by the National Institute of Standards and Technology (NIST), which recommends using standards to ensure the safety of communication between control systems. It is often used throughout the process of automating substations. The different possible attacks that may be attempted against a SCADA system are detailed in Table I, along with the cryptographic countermeasures that are recommended to ward off such assaults.

TABLE I: SCADA COMMUNICATION ATTACKS AND CRYPTOGRAPHIC METHODS

Types of Attacks	Cryptographic Solutions
An assault on the reliability of the data	The following are some examples of symmetric key algorithms: AES, DES, TDES, RSA, and ECC. The SHA-1 and SHA-2 algorithms are used for hashing data.
An assault on the authentication system	Implementations of HMAC and symmetric digital signature schemes
An assault on the privacy of the information	There are symmetric and asymmetric key algorithms, as well as asymmetric digital signature techniques.
Non-repudiation of Responsibility	Infrastructures for the generation of asymmetric digital signatures

It is possible to put an effective stop to these attacks by using strategies that are based on symmetric and asymmetric keys. The following is a description of the two most major aspects of SCADA communication in which asymmetric key cryptography is required:

❖ **The Terms Encryption and Decryption**

Encryption and decryption are the two fundamental cryptographic methods that are used in order to guarantee safe communication and prevent unauthorised access to data. It is projected that the vast majority of the hardware used in SCADA systems will be outfitted with at least basic knowledge of cryptography, which will likely include support for symmetric as well as asymmetric key cryptography. In spite of the fact that symmetric key encryption is superior in speed and takes less resources than its asymmetric counterpart, it is not possible to use it to verify the message. This is despite the fact that symmetric key encryption is superior in both of those areas. Another one of these systems' drawbacks is the arduous nature of key management in large-scale implementations. As a direct result of this, an asymmetric key algorithm is need to be used.

❖ **Authentication**

Authentication is the process of establishing that a person or thing is who or what it claims to be. This may apply to verifying the identity of the sender of a message or the person or thing that an item claims to be. It is necessary to have a crucial identifying technique in order to prevent attacks on the dependability of the data. In order to successfully support multicast communication, the authentication mechanisms for SCADA systems need to be highly effective, fault-tolerant, and attack-tolerant. In addition, they must be able to handle faults. Digital signature systems and keyed-hash message authentication codes, commonly known as HMAC, are the two types of authentication techniques that are used in SCADA the majority of the time. SCADA systems make use of multicast for a variety of purposes, including monitoring, the dissemination of information, and the protection of information. One example of this kind of application is found in the realm of substation communication systems. According to the most recent security standard for substation communication, known as IEC 62351, asymmetric digital signatures are recommended as the method of multicast authentication that is both the most user-friendly and the most practical. When HMAC is employed in multicast transmission, it does not give authentication of the data's origin, which is the primary reason why this is a problematic situation. Because everyone in a group context uses the same HMAC key (symmetric key), it is difficult to determine who the sender is with any degree of certainty. Even though HMAC provides protection at the group level, data-origin authentication cannot be performed. An asymmetric digital signature makes use of two different keys, but only one of those keys is ever shared with the recipient of the signature. Authentication of the data source is made possible by these signatures, making them an excellent choice.

4. Analysis and Interpretation

Examining the performance characteristics of NTRU, RSA, and ECC may be accomplished by first developing the calculation algorithms with the assistance of the free Java package Bouncy Castle 1.47, and then comparing the times at which the tests were carried out. In this way, the algorithms can be compared side by side. We merged the Cacao Java Virtual Machine with the Open JDK-7 development kit in order to speed up the execution. We did our testing on a Raspberry Pi operating Linux at 700 MHz and an Intel(R) Core (TM) i3 CPU operating at 2.27 GHz so that we could compare the respective levels of performance achieved by each CPU. In the first experiment, a comparison of the run times of NTRU and RSA was carried out by using keys of varying length for each of the three fundamental cryptographic primitives. The generation of keys, encryption, and decryption are all examples of these primitives. We took a peek at a random 32-byte message that was generated by the computer. Tables 2 and 3 provide the

results obtained with a device powered by a Raspberry Pi and a system powered by Intel, respectively.

TABLE 2: A COMPARISON OF THE SPEEDS OF KEY GENERATION, ENCRYPTION, AND DECRYPTION USING AN INTEL CORE @ 2.27GHZ

Asymmetric Algorithm	Key Generation (ms)	Encryption (ms)	Decryption (ms)
RSA-2048	91.53	0.53	3.08
RSA-3072	236.67	0.61	8.51
NTRU-439	9.29	0.29	0.29
NTRU-743	11.96	0.36	0.27

When it comes to the generation of asymmetric keys, the data indicate that RSA performs quite badly in both scenarios. This is the case. In addition, it was shown that NTRU decryption (private key operation) performed several times quicker than its RSA counterpart for the same level of security (RSA-2048 may be compared to NTRU-439, and RSA-3072 may be compared to NTRU-743). This was accomplished while maintaining the same level of safety. This was accomplished without compromising the standard of safety that was in place.

TABLE 3: A COMPARISON OF THE RATES OF ENCRYPTION AND DECRYPTION FOR KEY CREATION USING THE RASPBERRY PI'S 700 MHZ PROCESSOR

Asymmetric Algorithm	Key Generation (ms)	Encryption (ms)	Decryption (ms)
RSA-2048	25367.25	76.3	11236.38
RSA-3072	718569.35	173.36	3698.25
NTRU-439	1236.31	16.38	20.36
NTRU-743	2865.46	159.38	65.36

Encryption happens far more quickly than decoding does because RSA uses a precisely calculated public exponent (0x10001) to reduce the amount of processing work that is required. Even at this late date, the rate at which NTRU encrypted data was two to three times faster than that of RSA. In SCADA systems that are required to operate within a real-time constraint, using NTRU as an encryption approach would be the most effective course of action, as shown by the results. In addition, the performance of RSA, ECC, and NTRU digital signature algorithms was evaluated with the help of Java. The results of a number of experiments were compiled to provide the data that is shown in Table 4, which makes comparisons between the average signature and verification times for various procedures. When compared to RSA and ECC, the NTRU signature technique unquestionably requires much less time than the other two. As a result, it is a preferable choice for SCADA systems that need authentication services. This is as a result of the difficult nature of RSA and ECC. A more optimised version of NTRU written in C may be able to conduct operations at a faster rate when compared to the optimized version of its predecessors. This is because C allows for more optimization.

TABLE 4: COMPARISON OF THE SPEED OF SIGNING AND VERIFYING ON THE RASPBERRY PI AT 700 MHZ AND THE INTEL CORE AT 2.27 GHZ

Asymmetric Algorithm	Signing speed (ms)		Verification Speed (ms)		Total Digital Signature Speed (*ms*) (~)	
	Intel Core	***Rasp. Pi***	***Intel Core***	***Rasp. Pi***	***Intel Core***	***Rasp. Pi***
RSA-2048	41.36	1325	1.65	49.36	43	1369
RSA-3072	65.36	3869.8	1.88	85.65	66	4089
ECDSA-224	11.32	439.6	5.69	365.3	15	775
ECDSA-256	25.36	936.5	6.3	458.35	25	1365
NTRU-439	5.36	407.3	4.23	207.36	10	609
NTRU-739	6.32	536.8	6.35	369.24	15	958

5. Result and Discussion

The NTRU approach, which stands for "N-th degree truncated polynomial Ring Unit," is now being evaluated for its potential usefulness as a cryptographic answer for SCADA systems. The distinctive qualities of the technique, such as its high resistance to breaches carried out by means of quantum computing and its modest requirements in terms of processing power, are what are driving the interest in this approach. When NTRU is employed in SCADA networking applications, the impacts that are described below are potential outcomes that may occur. According to the information that was provided earlier, NTRU is a pragmatic cryptographic technology that has the potential to be used to the protection of SCADA applications when they are employed in networking.

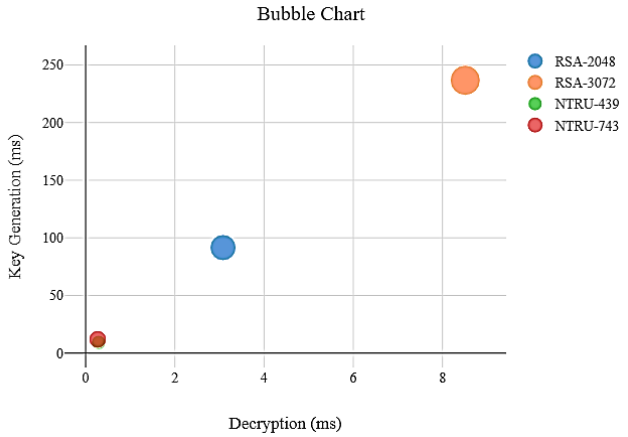

FIG 3: PERFORMANCE METRICS FOR CRYPTOGRAPHIC ALGORITHMS

Figure 3 illustrates the performance characteristics of a wide variety of different cryptographic algorithms, including RSA-2048, RSA-3072, NTRU-439, and NTRU-743, amongst others. These characteristics, which are specified in milliseconds (ms) for encryption, decryption, and key formation, are shown graphically in the following image. There is a single data point representing each technique, and its frequency is equal to one. The "Decryption (ms)" section makes it abundantly clear that the decryption of RSA-2048 takes approximately 3.08 milliseconds, the decryption of RSA-3072 takes approximately 8.51 milliseconds, and both NTRU methods, NTRU-439 and NTRU-743, offer noticeably faster decryption timings, with 0.29 milliseconds and 0.27 milliseconds, respectively. This information is readily apparent. In terms of "Key Generation (ms)," the construction of an RSA-2048 key takes the longest, measuring in at 91.53 milliseconds, while the development of an RSA-3072 key takes the longest, measuring in at 236.67 milliseconds. The production of keys takes a noticeably shorter amount of time using the NTRU-439 (9.29 ms) and NTRU-743 (11.96 ms) algorithms, respectively.The last part, under "Encryption (ms)," reveals that RSA-2048 encryption requires around 0.53 milliseconds, RSA-3072 encryption requires a little more time, 0.61 milliseconds, and both NTRU algorithms have rapid encryption rates, with NTRU-439 requiring 0.29 milliseconds and NTRU-743 requiring 0.36 milliseconds respectively.

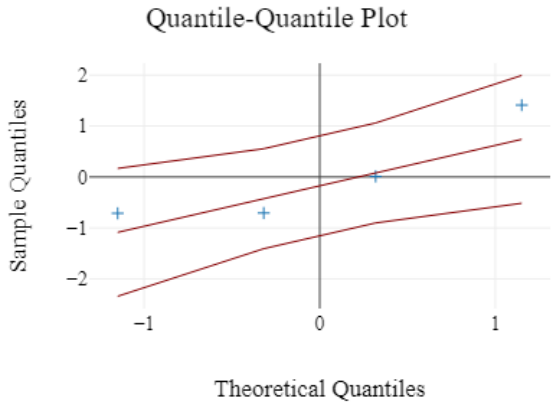

FIG 4: STATISTICAL TEST RESULTS FOR DATA DISTRIBUTION NORMALITY

In Figure 4, we can see that the Kolmogorov-Smirnov statistical test, the Shapiro-Wilk statistical test, the Anderson-Darling statistical test, and the Kolmogorov-Smirnov statistical test with the Lilliefors adjustment all have high p-values. This illustrates that the assertion that the data significantly deviates from a normal distribution is not supported by adequate evidence. This is shown by the fact that this sentence has no conjunctions. It is possible to draw this conclusion from the fact that there are no significant deviations from a normal distribution. As a consequence of this, it is reasonable to infer from the results of these tests that the data follows the properties of a normal distribution. This is essential in order to make use of a wide range of statistical methods and models.

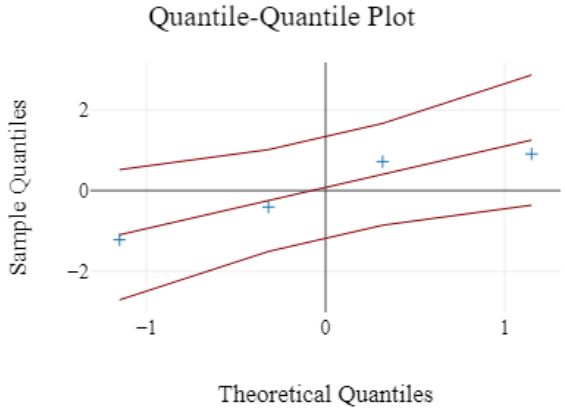

FIG 5: TESTS FOR NORMAL DISTRIBUTION OF ENCRYPTION (MS)

As can be seen in Figure 5, a number of statistical tests were carried out in order to establish whether or not a dataset exhibited normality. The results of the Kolmogorov-Smirnov test reveal a p-value of 0.26, which suggests that there is insufficient evidence to contradict the null hypothesis that the data have a normal distribution. This is because the null hypothesis states that the data have a normal distribution. The data seem to be regularly distributed, according to the result of the Lilliefors-corrected Kolmogorov-Smirnov test, which has a p-value of 0.26. This

finding verifies that the data are normally distributed. The fact that the Shapiro-Wilk test produces a p-value of 0.91 is yet another piece of evidence suggesting that the data may be reasonably fit into a normal distribution. The Anderson-Darling test, which determines whether or not the data significantly deviates from a normal distribution, ultimately produces a p-value of 0.37. This number verifies that the data does not considerably diverge from a normal distribution. Given the results of the tests that were carried out, these findings indicate that it is reasonable to conclude that the dataset follows a normal distribution.

❖ **Strong Security**

NTRU provides a high level of security against classic cryptographic attacks such as factoring and discrete logarithm problems. These techniques are well-known in the industry. Securing sensitive data and control orders in SCADA networks needs high security, which makes it difficult for unauthorised actors to edit or decode data. This is because good security costs a lot of resources.

❖ **Low Computational Overhead**

In contrast to other, more well-known public-key algorithms, such as RSA and ECC, NTRU has a far lower need for computing resources, which is one of its fundamental advantages. The effectiveness of NTRU is a significant advantage in SCADA settings when there are little available processing resources. It enables confidential communication without impairing the operational capabilities of SCADA apparatus.

6. Conclusions

In a previous post, we discussed how essential it is to protect SCADA communication, as well as how challenging it may be to employ conventional asymmetric key encryption techniques, such as RSA, in real-time systems that have limited hardware resources. In particular, we focused on the challenges that may be presented by these circumstances. In order to assure end-to-end security in SCADA systems and devices while still following to real-time limitations, an alternate asymmetric key cryptography approach is required. This method also offers a number of benefits. Based on the findings of this study, it is recommended that NTRU-based encryption and authentication be used in SCADA systems in order to solve problems with data integrity, secrecy, authentication, and non-repudiation. RSA and ECC are both outperformed by NTRU due to the fact that the latter does not need factorization or discrete logarithmic calculations. The performance of the asymmetric key techniques RSA, NTRU, and ECC was examined using hardware based on the Raspberry Pi computer and the Intel CPU. According to the findings, NTRU performs far better than RSA and ECC when it comes to the speed at which security is achieved.

References

[1] Anjula Gupta , et.al. “Cryptography Algorithms: A Review “ *International Journal of Engineering Development and Research*, Vol.2 No.2, (2014).

[2] Mini Malhotra et.al. “ Study of Various Cryptographic Algorithms”, *International Journal of Scientific Engineering and Research*, Vol.1, No.3, (2013), PP.77-88.

[3] Shashi Mehrotra Seth et.al,” Comparative Analysis Of Encryption Algorithms For Data Communication”, *International Journal of Computer Science and Technology*, Vol.2, No.2 (2011) pp.292-294.

[4] S G Suganya, Prasanna D, “Detection and Prevention of DDoS Attack Using Modern Cracking Algorithm”, *International Research Journal in Advanced Engineering and Technology*, Vol.2, Issue.3, Apr 2017.

[5] E. Thambiraja, G. Ramesh, Dr. R. Umarani, “A Survey on Various Most Common Encryption Techniques” *International Journal of Advanced Research in Computer Science and Software Engineering,* VOL. 2, Issue 7 July 2012, Page 226-233.

[6] Sumedha Kaushik, Ankur Singhal, “Network Security Using Cryptographic Techniques” *International Journal of Advanced Research in Computer Science and Software Engineering*, VOL.2, Issue 12 December 2012, Page 105-107.

[7] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." *Dr. Dobb's Journal*, March 2001.

[8] Pranay Meshram,Pratibha Bhaisare, S.J.Karale,”,comparative study of selective encryption algorithm for wireless adhoc network” ,IJREAS Volume 2, Issue 2 , in *International Journal of Research in Engineering & Applied Sciences*.

[9] Punita Mellu & Sitender Mali, “AES: Asymmetric key cryptographic System” *International Journal of Information Technology and Knowledge Management*, 2011, Vol, No. 4 pp. 113-117.

[10] Wenye Wang, Zhuo Lu., “Cyber Security in the Smart Grid: Survey and challenges”, Computer Networks: *The International Journal of Computer and Telecommunications Networking*, Vol.57 Issue 5, April, 2013.

[11] Martin Drahansky and Maricel Balitanas., “Cipher for Internet-based Supervisory Control and Data Acquisition Architecture,” *Journal of Security Engineering*, Jun, 2011.

[12] Aamir Shahzad and Shahrulniza Musa., “Cryptography and Authentication Placement to Provide Secure Channel for SCADA Communication”, *International Journal of Society (IJS),* Vol.6, Issue.3, 2012.

[13] PAN, S., LIU, X., XIE, N. and CHONG, Y., 2023. EG-TransUNet: a transformer-based U-Net with enhanced

and guided models for biomedical image segmentation. BMC Bioinformatics, 24, pp. 1-22.

[14] RAMYA SHREE, H.P., MINAVATHI and DINESH, M.S., 2023. An Automatic Nuclei Segmentation on Microscopic Images using Deep Residual U-Net. International Journal of Advanced Computer Science and Applications, 14(10),.

[15]] SAIDA, D. and PREMCHAND, P., 2022. Brain Tumor Identification using Dilated U-Net based CNN. International Journal of Computers, Communications and Control, 17(6),.

[16] SITANABOINA S.L. PARVATHI, BOLEM, S.C. and HARIKIRAN, J., 2023. Depth Invariant 3D-CU-Net Model with Completely Connected Dense Skip Networks for MRI Kidney Tumor Segmentation. Traitement du Signal, 40(1), pp. 217-225.

[17] [Bani Ahmad, A. Y. A. ., Kumari, D. K. ., Shukla, A. ., Deepak, A. ., Chandnani, M. ., Pundir, S. ., & Shrivastava, A. . (2023). Framework for Cloud Based Document Management System with Institutional Schema of Database. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(3s), 672–678.

[18] P. William, Anurag Shrivastava, Upendra Singh Aswal, Indradeep Kumar, Framework for Implementation of Android Automation Tool in Agro Business Sector, 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), 10.1109/ICIEM59379.2023.10167328

[19] P. William, Anurag Shrivastava, Venkata Narasimha Rao Inukollu, Viswanathan Ramasamy, Parul Madan, Implementation of Machine Learning Classification Techniques for Intrusion Detection System**,** 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), 10.1109/ICIEM59379.2023.10167390

[20] N Sharma, M Soni, S Kumar, R Kumar, N Deb, A Shrivastava, Supervised Machine Learning Method for Ontology-based Financial Decisions in the Stock Market, ACM Transactions on Asian and Low-Resource Language Information Processing.

[21] [Ajay Reddy Yeruva, Esraa Saleh Alomari, S Rashmi, Anurag Shrivastava, Routing in Ad Hoc Networks for Classifying and Predicting Vulnerabilities, Cybernetics and Systems, Taylor & Francis, 2023

[22] P William, OJ Oyebode, G Ramu, M Gupta, D Bordoloi, A Shrivastava, Artificial intelligence based models to support water quality prediction using machine learning approach, 2023 International Conference on Circuit Power and Computing Technologie

[23] J Jose, A Shrivastava, PK Soni, N Hemalatha, S Alshahrani, A Saleel, An analysis of the effects of nanofluid-based serpentine tube cooling enhancement in solar photovoltaic cells for green cities, Journal of Nanomaterials 2023

[24] K Murali Krishna, Amit Jain, Hardeep Singh Kang, Mithra Venkatesan, Anurag Shrivastava, Sitesh Kumar Singh, Muhammad Arif, Deelopment of the Broadband Multilayer Absorption Materials with Genetic Algorithm up to 8 GHz Frequency, Security and Communication Networks

[25] P Bagane, SG Joseph, A Singh, A Shrivastava, B Prabha, A Shrivastava, Classification of malware using Deep Learning Techniques, 2021 9th International Conference on Cyber and IT Service Management (CITSM).

[26] A Shrivastava, SK Sharma,Various arbitration algorithm for onchip (AMBA) shared bus multi-processor SoC, 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science, SCEECS 509330

[27] A. Gandomi, M. Haider, “Beyond the hype: Big data concepts, methods, and analytics”, *International Journal of Information Management,* vol. 35, no. 2, pp. 137-144, 2015.

[28] Shrivastava, A., Chakkaravarthy, M., Shah, M.A..A Novel Approach Using Learning Algorithm for Parkinson’s Disease Detection with Handwritten Sketches. In Cybernetics and Systems, 2022

[29] Shrivastava, A., Chakkaravarthy, M., Shah, M.A., A new machine learning method for predicting systolic and diastolic blood pressure using clinical characteristics. In *Healthcare Analytics*, 2023, 4, 100219

[30] Shrivastava, A., Chakkaravarthy, M., Shah, M.A.,Health Monitoring based Cognitive IoT using Fast Machine Learning Technique. In *International Journal of Intelligent Systems and Applications in Engineering*, 2023, 11(6s), pp. 720–729

[31] Shrivastava, A., Rajput, N., Rajesh, P., Swarnalatha, S.R., IoT-Based Label Distribution Learning Mechanism for Autism Spectrum Disorder for Healthcare Application. In *Practical Artificial Intelligence for Internet of Medical Things: Emerging Trends, Issues, and Challenges*, 2023, pp. 305–321

[32] Boina, R., Ganage, D., Chincholkar, Y.D., .Chinthamu, N., Shrivastava, A., Enhancing Intelligence Diagnostic Accuracy Based on Machine Learning Disease Classification. In *International Journal of Intelligent Systems and Applications in Engineering*, 2023, 11(6s), pp. 765–774

[33] Shrivastava, A., Pundir, S., Sharma, A., ...Kumar, R., Khan, A.K. Control of A Virtual System with Hand Gestures. In *Proceedings - 2023 3rd International Conference on Pervasive Computing and Social Networking, ICPCSN 2023,* 2023, pp. 1716–1721

[34] A. P. Srivastava, P. Choudhary, S. A. Yadav, A. Singh and S. Sharma, A System for Remote Monitoring of

Patient Body Parameters**,** International Conference on Technological Advancements and Innovations (ICTAI), 2021, pp. 238-243,

[35] ELLOUMI, N., SLIM, B.C., SEDDIK, H. and NADRA, T., 2023. A 3D Processing Technique to Detect Lung Tumor. International Journal of Advanced Computer Science and Applications, 14(6),.

[36] EL-MELEGY, M., KAMEL, R.M., MOHAMED ABOU EL-GHAR, NORAH, S.A. and EL-BAZ, A., 2023. Kidney Segmentation from Dynamic Contrast-Enhanced Magnetic Resonance Imaging Integrating Deep Convolutional Neural Networks and Level Set Methods. Bioengineering, 10(7), pp. 755.

[37] GE, Z., ZHANG, Z., SHI, L., LIU, S., GAO, Y., ZHOU, Y. and SUN, Q., 2023. An Algorithm Based on DAF-Net++ Model for Wood Annual Rings Segmentation. Electronics, 12(14), pp. 3009.

[38] HAM, S., KIM, M., LEE, S., WANG, C., KO, B. and KIM, N., 2023. Improvement of semantic segmentation through transfer learning of multi-class regions with convolutional neural networks on supine and prone breast MRI images. Scientific Reports (Nature Publisher Group), 13(1), pp. 6877.

[39] JUNG, Y., KIM, S., KIM, J., HWANG, B., LEE, S., EUN, Y.K., KIM, J.H. and HWANG, H., 2023. Abdominal Aortic Thrombus Segmentation in Postoperative Computed Tomography Angiography Images Using Bi-Directional Convolutional Long Short-Term Memory Architecture. Sensors, 23(1), pp. 175.