A Residue Number System and Secret Key Crypto System Review in Cyber Security

Akanni Gabriel A.,
Kwara State College of Education
(Tech), Lafiagi, Kwara State

Eseyin Joseph B.
ICT Directorate, University of Jos,
Jos, Nigeria

Kazeem A. Gbolagade
Department of Computer Science
Faculty of Library & Information
Technology, Kwara State University, Malete, Ilorin

Abstract:- More people are embracing technology today because of the way we live, and they use it for both electronic banking and shopping. At the same time, knowledge protection has become more problematic. Along with the increased use of social media, online crime, often known as cybercrime, has become more and more predominant. The field of information technology places a high priority on data security. Information security is one of the most significant issues facing the globe today. When thinking about cyber security, we first take into "cybercrimes," which show considerable daily growth. To stop this type of cybercrime, various governments and corporations take various precautions. Numerous steps have been taken to protect against it, but many people are also extremely concerned. This paper briefly reviews the most up-to-date structures of the new technology's potential threats to cyber security. It also emphasizes advancements that affect cyber security, philosophies, new cyber security technology, and the nomenclature of Residue Number System (RNS) components for the design of secret key cryptography. The rapidity of RNS to binary conversion administers the moduli set in RNS, allowing for the efficient performance of operations like comparison, scaling, sign recognition, and fault correction.

Keywords:- *Cyber security, cybercrime, RNS, secret key, cyberassult and CRT.*

I. INTRODUCTION

The march of digitization has resulted in the gradual storage of sensitive data in all spheres of life, including healthcare, learning, trade, etc. Security is the process of guarding against physical damage or theft of digital data while maintaining its confidentiality and accessibility, yet as technology advances swiftly, cybercrime rates increase as well, both in frequency and complexity. The use of poor software, out-of-date security measures, and flawed programming. The explanations for this sharp rise in cybercrime include simple accessible virtual chopping tools, a deficiency of public consciousness, and significant cash gains. To find the target's vulnerabilities and subsequently attack the victim, technical attackers develop more powerful attack tools.

As a result, new, challenging-to-detect threats are emerging in various versions. The increased reliance on the internet in many aspects of life, the massive amounts of data generated by virtual infrastructures, and the subsidiarity of data warehouses have all contributed to the creation of active safety algorithms. The dynamic fauna of cyber-crime makes it challenging to manage and steer clear of new dangers. The most complex and difficult challenge is securing cyberspace because advanced threats are so prevalent there. Therefore, it is important to comprehend the concepts behind security defensive mechanisms, different approaches, and contemporary problems in the turf of data protection.

- Cybercrime remains the name given to theft and other crimes that include the use of a computer. The US Department of Justice has broadened the explanation of cybercrime to embrace act that keeps evidence on devices. Cybercrimes are crimes committed using computers, such as the dissemination of computer viruses and network intrusions, it also consists of PC based versions of traditional criminalities like larceny, pestering, coercion, and intimidation. In simple terms, cybercrimes are frequently offences executed utilizing a computer and the net to snip someone's distinctiveness, vend them to victims of smuggling or stalking, or mess up operations using destructive software. As technology advances, cybercrimes might also increase because knowledge now affects so many people's lives.
- Cybersecurity: Any organization should continuously be concerned with privacy and information protection as their top security priorities. In the very digital or virtual-specific world in which all the records are stored, square measures are preferred. Despite providing a secure milieu for users to communicate with relatives and family, fraudsters also use these platforms to acquire private data.

II. LITERATURE REVIEW

Jang-Jaccard, Julian [1] Strengthening protection of critical information substructure and cyber security are vital for the safety and fiscal success of any country. An innocuous internet has greatly aided the creation of new services and governmental policies (and protecting Internet users). Lee, H., et al. [2]. Key loggers are a common type of raiding tool that is simple to use online and logs all keyboard inputs made by users. It is one of many attachment methods that have surfaced in the past. D. Mellado, Mouratidis, e tal [3]. The SPL has not been investigated in the field of protection.

The majority of techniques focus on adding safety requirements or SPL features. Since the beginning of the product line's production, there have been many approaches to managing variability and safety standards. Anwar, Mohsin, e tal [4] The question in the realm of cyber security is whether well-established feature model techniques can be used or modified for cyber security. A strategy is put forth to improve the creation of secure software product lines and their derivative products (SPLs). VeenooUpadhyay [5]. The wizard prompts the user to "identify" a few certain friends with privacy to routinely grant privileges to new user friends. His machine-learning classifier is developed using this response. The strategy was inspired by the understanding that real operators are conscious of their privacy practices and that friends may be able to see which information they use and repeat in other friends' settings based on an implicit set of criteria. Yim, K [6]

The core area of this procedure is to identify keyboard data attack methods while preventing the user from disclosing the actual data entered. The guard, in particular, a keyboard input occurrence is required to protect the user's true keyboard data intake by filtering the keyboard data generation and delivering unsystematic keyboard data. Nichole Tresa Sadath Cyriac Lips [7] The perpetrators of a cyber bout are also discussed, along with the primary procedures they employ to succeed. It elucidates the general framework of cyber assault, and its stages, besides its effects on the fiscal structure. M. Liakat Ali [8] The paper focuses on the most recent cyber safety tactics, drifts, and other cyber security principles. This study provides a quick outline of the cyber security issues caused by contemporary technological and innovative advances. Kutub Thakur [9] The terms "cyber security" and "knowledge security" were used interchangeably; however, as time has gone on, it has come to recognize the importance of humans in the safety process. However, since it touches on the ethical foundation of society as a whole, a discussion like this one on cyber safety has significant ramifications. Different approaches and concepts are created to address this issue of cyber defense.

J.li [10] appraised firewall concerns and the best approach to set up routing tables to minimize the maximum firewall rule established, preventing performance bottlenecks and limiting security breaches. Since these issues of the heuristic method have been suggested because they are NP-complete. to employ simulation to demonstrate how functioning an algorithm is. A total of two significant contributions have been made. Cybersecurity Methodologies by utilizing new methods, cyber assaults in cyberspace have the potential to increase. To exploit brand-new technical flaws, cyber felons will most usually update the malware signatures that are currently in use. In other cases, they genuinely gaze for exclusive features of cutting-edge technology to spot vulnerabilities in malware insertion.

Using these new technologies, cyber scoundrels are easily and swiftly getting access to a large number of people by leveraging the rapidly emergent Internet and its millions and billions of active users.

III. PASSWORD AND ACCESS CONTROL SECURITY

Using the username and password security is a quick and simple way to safeguard confidential information and demesne privacy. This kind of haven protection is among the utmost significant virtual security initiatives.

- **Data Authentication:** Up until the information is transferred, it must be proven that it came from a reliable source and was not altered. A present from the competing virus program installed on PCs is frequently used to validate these documents. To defend devices from infections, a package of genuinely anti-virus software is more crucial.
- **Malware Scanners:** A software program that, on occasion, checks the entire system's files and documents for viruses or other hazardous code Trojan horses, worms, and viruses are frequently used in this industry to sort and classify examples of malicious software systems as malware.
- **Firewall:** A firewall is a part of hardware or software that stops hackers, viruses, and worms from getting online and accessing your computer. Using a firewall, it looks at each message that enters and rejects any that don't adhere to the standards for universal message security. Firewalls are essential for detecting malware.
- **Social Media's Role in Cybersecurity**: Interactive businesses are needed in today's modern world since there is a greater requirement for securing personal data in complex environments. Social media is crucial for both personal cyberattacks and cyber security. Because more employees are using social media, the threat of an attack is intensifying. Since the majority use social networking sites or other forms of social media. This has provided a tremendous platform for fraudsters to steal vital information and breach personal data every day. Nowadays, it's quite simple to seepage personal information, so organizations need to be definite to identify, respond at the moment, and stop breaches of any kind as rapidly as imaginable. Users can easily give their personal information to these social media sites, which hackers can subsequently use. As a result, people must take appropriate security measures to guard against the misapplication and forfeiture of data on social media platforms.

IV. CURRENT CYBER SECURITY TRENDS SURVEY ISSUES

Cybersecurity entails being aware of several cyber pressures and putting guard plans in place to protect the availability, credibility, and secrecy of IT technology. Malware is frequently recognized as the main technique employed by evil actors to get beyond internet security processes. The most common type of attack that is placed onto a device without the owner's consent is called malware. A computer can become infected by malware, which includes in addition to propagating from infected devices and fooling users into opening malicious files, viruses, worms, Trojan horses, spyware, and bot executables can also be distributed electronically. suspicious files, or attracting users to harmful websites. Malware can infect a system by installing itself onto a USB device that has been plugged into a compromised computer. This happens in more real-world instances of malware infection.

The computational logic and embedded systems of equipment and gadgets can transmit malware. At any point in a device's life cycle, malware can be introduced. Malware can attack end users, servers, networking hardware (such routers, switches, etc.), and even SCADA-style process control systems. There is currently a lot of anxiety online about the complexity and growth of malware. The attacks' goal is to trick their victims into thinking they are communicating with a reliable individual by email, text, or increasingly by phone to obtain sensitive information including card information, social security numbers, usernames, and passwords.

- **IoT Ransom ware:** The Internet of Things includes many network-connected devices, including domestic appliances and service sensors. Although they hardly ever store sensitive information on their own devices, refrigerators and temperature control equipment may be exploited as captives and targets by sniffers to steal data from backend systems like those in power supply and communication infrastructure.
- **Tougher Global Regulations**: The General Data Protection Regulations for Europe (GDPR), which went into effect in May 2018, were developed to protect European people' privacy rights and to ensure that stronger international regulations are followed at all times or risk harsh fiscal consequences.
- **Cyberattacks on Mobile Devices:** According to latest RSA enquiry, "80% of fraudulent mobile transactions" have increased exponentially in 2018 thanks to mobile application scams since 2015. As mobile strategies permeate every aspect of our individual and skilled lives, risk acuities have also increased.
- **Increased investment in automation:** Organizations are embracing automation technologies because it frees up overworked cyber security workers to focus on challenging problems rather than repetitive, menial tasks. Recent Ponemon Institute research found that 79% of participants said they utilize frameworks and technologies for security automation, and 50% said they plan to use them in their enterprises. In these circumstances, the first method of data protection offers the strongest resistance against cyber bouts like database fraud and fitness, which can have a significant negative impact on a company. Although it might increase productivity, skills and knowledge are still needed to reduce the danger of cybercrime.
- **Prevention strategies for cybercrimes:** The most recent developments in digital safety are 1. Both businesses and cyber security expertise are changing. 2. Protection is the top priority in the cloud. 3. Reorient your responsiveness away from security and deterrence 4. Production facilities cope with the data plus application security for the foreseeable future. Cybercrime cannot be detected in digital environments solely by technology means; also, legal actions, organizational modifications, international cooperation, and capacity building were required.

V. RESIDUE NUMBER SYSTEM

A Residue Number System (RNS) represents a great number using a group of slighter integers so that computation can be done more efficiently. It operates according to the Sunzi Suanjing, a mathematical principle based on the Chinese remainder theorem of modular arithmetic, which dates back to the 4th century AD. Utilizing the residue number scheme is not weighted. This system differs significantly from weighted number systems like the binary and decimal ones. Because each result digit is a function of just one digit from each operand and is hence independent of all other digits, residue arithmetic operations like addition, subtraction, and multiplication are by their very nature carry-free. [11]

This capability considerably boosts the processing speed, a crucial component in applications for digital signal processing. The essential ideas of how numbers are represented in residue systems, fundamental arithmetic operations, and how residue numbers are transformed into weighted number systems utilizing CRT and MRC processes are all covered in this section.

A. The residue representation's description

In a fixed-radix scheme, the base is used to quantify the number system. Declaring the base, which entails an n-tuple of integers rather than a solitary integer, defines RNS. As a result, a set of numbers m_1, m_2, m_n, where each discrete element is referred to as a modulus, determines the radix of an RNS. [12]

The residue representation of a number x is another n-tuple, (x1, x2,..., xn), where xi is integers that can be designated by a set of n equations for each given base.

$$g = h_i m_i + g_i \ldots \text{ for } I = 1,2,\ldots,n$$

and q_i is an integer so selected that $0 \leq g_i \leq m_i$. It is distinct that h_i is the integer value of the quotient ^{g}. The amount *xi* is the least positive (integer) m_i remainder of the division of g*x* by m_i, and is termed the residue. The residue is the least positive remainder when the number G is divided by the modulus mi. [1,4,8]

g*x* modulo m_i or $|g|_{mi}$, often stated as g*x mod mi.*

For Example

For G = 57 and m1 = 4 and m2 = 5 we find the residues r1 and r2 regarding the moduli m_1 and m_2, correspondingly as follows:

57 mod 4 = 1 since 57 = 4 x 14 + 1

57 mod 5 = 2 since 57 = 5x 11 + 2

The ith residue of g is another name for the number gi. Here, g can be any integer and is not required to be positive. The quotient of g will also be negative if g is negative. |g|mi must be positive according to mi definition. If the number is inside the dynamic range, the residual depiction of the number is identifiable. The dynamic range for positive numbers g is 0 to M - 1, where M is the sum of the moduli. When working with both positive and negative values, the dynamic range ranges from

$-^{(M-1)}$ to $^{(M-1)}$ for *M* odd, and from

$-^{(M-1)}$ to $^{(M-1)}$ for *M* even

2

This means that a residue numeral system is defined by a set of N integer constants, often known as the moduli: m_1, m_2, m_3,..., m_N..

Let M signify the least Significant number among all the mi. The residue numeral system can represent any unsystematic number X lower than M as a collection of N smaller integers, where xi = X modulo mi denotes the residue class of X to that modulus.

The moduli should be pairwise coprime for representational efficiency, which means that no modulus should share a factor with any other.[10]

For example: Consider this two RNS,(i) {2 ,3 ,5 } and (ii) {2 ,3 ,4 }

The moduli in the 2, 3, and 5 moduli sets are largely prime. All numbers between 0 and 29 have a specific RNS representation. The RNS representation repeats itself outside of that range. For instance, the RNS representation of 30 and 0 are identical. Since 2 and 4 have a common divisor of 2, the moduli in the moduli-set of the second RNS, 2, 3, and 4, are not relatively prime. Since RNS (4|2) has no coprime moduli per LCM of 4 then produce 8, different values smaller than the product have identical representation [12]. The dynamic range is not fully utilized due to the RNS representation repeating itself at the number 12. To ensure discrete representation within the dynamic range, it is crucial to use reasonably prime moduli for the RNS.

B. Residue Number to Weighted Number System Conversion

The transition from the RNS to a weighted number system is a significant step in the design of RNS-based systems. The two primary conversion techniques are the Mixed Radix Conversion operation and the Chinese Remainder Theorem. Chinese Remainder Theorem.

The following is the formulation of the Chinese Remainder Theorem (CRT) [11]:

Given the residue representation and a system of pair-wise relatively prime moduli (m_1, m_2, m_3, mn), (r_1, r_2,..., r_n) of a number X (r_1 = |x|mi), the following relation exists between the number and its residues:

$$|x|_{m} = \sum_{i=1}^{n} ri \mid m_1^{-1} \mid mimi \mid m$$

M =, where M is the product of the mi's. The modular reduction on the left side can be skipped if the values involved are restricted so that the final value of X falls within the dynamic range.

Following the preceding equation, there are three basic steps needed to implement the CRT:

- Getting the inverses of the mi's.
- Operations that multiply and accumulate
- Modular lowering

Since there is no general method to obtain m_i^{-1} using any standard Equation the best way to implement it is to save the constants Xi in = $\lfloor m_i^{-1} \rfloor mi\, Mi$ in a ROM. These constants are then multiplied with the residues (r_i) and added using a modulo M adder.

C. Mixed Radix Conversion Process

Arithmetic operations for modulo M are essential for the Chinese Remainder Theorem. The CRT-based residue converters are consequently extremely complex. Contrarily, the Mixed-Radix Conversion procedure just calls for arithmetic calculations for modulo mi, simplifying all operations in comparison to CRT. The MRC procedure uses a mixed-radix approach to express the value of x. This number X can be written in mixed-radix form as follows given a set of pair-wise relatively prime moduli m1, m2, m3,..., mn and a residue representation r1, r2,..., rn of some number X in that system, where ri = |x|mi: [1,4 .5]

$$X = \{z_1, z_2 , z_3, \ldots, z_n\}$$

Where

$$X = z_1 + z_2 m_1 + z_3 m_1 m_2 + \ldots\ldots\ldots\ldots\ldots z_n m_{n-1} m_{n-2} \ldots\ldots\ldots m_{n-1}$$

And $0 \leq zi \leq ri$

A relationship between a non weighted, non- positional RNS and a weighted, positional mixed-radix system is established via the Mixed-Radix Conversion (MRC). Obtaining the values zi is all that is necessary to execute the reverse conversion.

$$z1 = r1$$

$$z_2 = |(r2 - z1)| m_1^{-1} \mid m_2 \mid m_2$$

$$z_{3} = |((r3 - z1)| m_1^{-1}|_{m3 - z2)} |m_2^{-1}|m3|_{m3}$$

$$z_{n} = |((\ldots(rn - z1)| m_1^{-1}|_{mn - r2)} |m_2^{-1}|m3 - \ldots\ldots\ldots zn\text{-}1)| m_n^{-1} |m_n|_{mn}$$

Given the Mixed Radix Digits Z1, $0 \leq zi \leq ri$ any positive number in the intermission [0, $\coprod_{i=1}^{n} ri - 1$ can be represent.

D. Selecting Moduli

The selection of moduli and the quantity of moduli affect both the dynamic range and the involvedness of the resulting circuitry. There are precise considerations that is a requisite to choosing moduli. The points are as follows: [12] Moduli must be prime to one another.

All other moduli should be made equivalent in scope to the leading one since the magnitude of the largest modulus decides how swiftly arithmetic operations are performed.

The most common moduli set, according to a literature review, is (2^n-1), 2^n, and (2^n+1). [11]

VI. CRYPTOGRAPHY

There are many distinct learning areas within the modern topic of cryptography. As follows:

symmetric-key cryptography, which encrypts and decrypts data using only one key.

The sorts of encryption techniques known as symmetric-key cryptography assign the same key to the sender and the recipient. Up until June 1976, this was the only type of encryption that was widely understood. Anyone can encrypt messages using the public key of asymmetric key encryption, but only the owner of a matching private key is able to decrypt them. To guarantee the security of the system, the private key must be kept hidden. [10] Asymmetric cryptography, or public-key cryptography, is a kind of communication in which parties exchange messages that are only readable by one another.

Each user in public key cryptography has two cryptographic keys which are an open key and a personal key.

While the public key can be shared publicly and utilized by other users, the private key has been maintained as secret. The recipient's public key is used to encrypt the inbound messages, and only their corresponding private key may be used to decrypt them. Although the keys are theoretically related, it is impossible to deduce the user's private key from the commonly used public key. Block ciphers and stream ciphers are both used to as tool for symmetric key ciphers. The input form employed by a stream cipher, blocks of plaintext, is encrypted by a block cipher as divergent to individual characters. Advanced Encryption Standard (AES) and Data Encryption Standard (DES) (AES) are block cipher designs that the US government has certified as cryptography standards.

It safeguards remote access and is utilized in a variety of applications, such as ATM encryption and email privacy. [10] Unlike "block" ciphers, which combine the plaintext bit-by-bit or by-character, stream ciphers produce an illogically long stream of key material. In this way, they resemble one-time pads. During a stream cipher's operation, a concealed internal state that is used to construct the output stream changes. The key management required to use symmetric ciphers securely is a notable drawback. Ideally, each unique brace of communication must have a stake as a distinctive key, and possibly individual ciphertext is also swapped. As the square of the number of network members, more keys are needed. To keep them all consistent and secret, this calls for a sophisticated key management system. When a secure channel does not already exist between two communicating parties, the difficulty of generating a secret key between them creates a significant issue. [13].

A. USES

Military forces and governments have historically utilized encryption to enable covert communication. Information protection is currently frequently employed in many different types of civilian systems. Data that is stored "at rest," such as on computers and storing devices, can be protected via encryption. There have existed several stories in recent years of backup disks or laptops being lost or stolen and exposing sensitive information, including client details. Such files are better protected if they are encrypted at rest if physical protection measures are unsuccessful. Digital rights management systems, which prevent the unauthorized use or duplication of copyrighted information and safeguard software, are another, slightly different example of using encryption on data at rest. against reverse engineering [12]. Encryption is used to secure data transfer across networks (such as the Internet, for instance), mobile phones, wireless microphones, wireless intercom systems, Bluetooth devices, and automated teller machines in banks. There have been numerous instances of data being intercepted while in transit in recent years. [12]. To prevent unauthorized users from listening in on network traffic, data ought to be encoded when being transported transversely within the networks.

VII. CONCLUSION

Due to the enormous growth in Internet entree, the development of Internet devices, population progression, and wide-ranging internet use, extremely sensitive personal data is recurrently shown online with diminutive cognizance of the consequences of information leaking. We believe that concerns over end-user privacy will grow as the amount of information available online expands in the coming years. Usability concerns are also becoming more and more important as a way to spontaneously learn about and apply end-user-oriented safety techniques devoid of challenging or significant learning curves to safeguard the data. Innovative updates that fix current security and confidentiality issues are used to build up the community's cyber safety practices. Some have confidence in this novel approach has nosedived and won't be able to satisfy the impending needs because the original Internet was developed in a rather diverse setting from how it is used nowadays. Instead of referring to the current computing system or the future, it is suggested to start again to enhanced the emergent demands of the future. In the subject of cryptography, where The most frequent operations in RNS arithmetic are addition and multiplication, but it has a wide range of uses. Each digit of the output is independent of all other digits since it only depends on one digit from each operand. Addition, subtraction, and multiplication are examples of residue arithmetic operations that are inherently carry-free. This capability significantly improves processing speed, which is a key factor in applications for digital signal processing.

REFERENCES

[1.] Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.

[2.] Lee, H.; Lee, Y.; Lee, K.; Yim, K. Security Assessment on the Mouse Data using Mouse Loggers. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Asan, Korea, 5–7 November 2016

[3.] Mellado, D.; Mouratidis, H.; Fernández-Medina, E. Secure Tropos Framework for Software Product Lines Requirements Engineering. Comput. Stand. Interfaces 2014, 36, 711–722

[4.] Mohsin, M.; Anwar, Z.; Zaman, F.; Al-Shaer, E. IoT Checker: A data-driven framework for security analytics of Internet of Things configurations. Comput. Secure. 2017, 70, 199–223

[5.] Veenoo Upadhyay, SuryakantYadav Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349-2058, Volume-05, Issue-07, July 2018

[6.] Yim, K. A new noise mingling approach to protecting the authentication password. In Proceedings of the 2010 International Conference on Complex, Intelligent and Software Intensive Systems, Seoul, Korea, 30 June–2 July 2012

[7.] Nikita TresaCyriacLipsaSadath Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions 2019 4th International Conference on Information Systems and Computer Networks (ISCON) GLA University, Mathura, UP, India. Nov 21-22, 2019

[8.] MdLiakat Ali Kutub Thakur Beatrice Atobatele Challenges of Cyber Security and the Emerging Trends BSCI’19, July 8, 2019, Auckland, New Zealand

[9.] Kutub Thakur1, Meikang Qiu2∗, Keke Gai3, MdLiakat Ali4 An Investigation on Cyber Security Threats and Security Models 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing 978-1-4673-9300-3/15

[10.] J. Li. The research and application of multi-firewall technology in enterprise network security. Int’l J. of Security and Its Applications, 9(5):153–162, 2015

[11.] K.A. Gbolagade, S.D. Cotofana, A residue-to-binary converter for the {2n+2, 2n+1, 2n} moduli set, in *Proceedings of 42nd Asilomar Conference on Signals, Systems Computers*, pp. 1785–1789 (2008)Google Scholar

[12.] Eseyin, Joseph B, Gbolagade, Kazeem A (2019). A residue number system-based data hiding using steganography and cryptography. KIU Journal of Social Sciences, [S.l.]. 2019;5(2):345-351. July. ISSN 2519-0474.

[13.] *Menezes, A. J.; van Oorschot, P. C.; Vanstone, Scott A. (1997). Handbook of Applied Cryptography. ISBN 0-8493-8523-7.*