Tony Blair Institute for Global Change
Trinity University, Lagos, Nigeria
Harmarth Global Educational Services
FAIR Forward – Artificial Intelligence for All
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
Society for Multidisciplinary & Advanced Research Techniques (SMART)

Accra Bespoke Multidisciplinary Innovations Conference (ABMIC)

Development Of An Adaptive Hyper-Elliptic Encryption With Cellular Automata Model For Distributed Systems

Raheem, M.M. & Adeyemo, A.B.
Department of Computer Science
University of Ibadan
Ibadan, Nigeria

ABSTRACT

Today we see proliferation of micro- controller embedded devices in the world that one can hardly imagine how the world will be without all these devices. Every homes and corporate entities uses micro-controllers embedded devices such as electronic passports, contactless banking cards, access control tokens, car keys, phones, televisions and even small appliances like toasters at their own conveniences. There is however less emphasis on the potential security and privacy risks one get exposed. To address this issue, this paper sets out a research agenda for the development of an adaptive hyper-elliptic encryption with cellular automata model for distributed systems

Keywords: Security, Adaptive, Hyper Elliptic Encryption, Cellular Automata, Distributed Systems

Proceedings Citation Format
Raheem, M.M. & Adeyemo, A.B. (2022): Development Of An Adaptive Hyper-Elliptic Encryption With Cellular Automata Model For Distributed Systems. Proceedings of the 31st Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Ghana. 1st – 3rd June, 2022. Pp 155-166, www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS/ABMIC2022P17

1. BACKGROUND TO THE STUDY

In the information age, we do business and exchange information with people who may have conflicting interests with us in this modern information-driven society. While Cloud computing which virtualized almost all the necessary resources provide scalable and flexible IT functionalities to external customers using Internet technologies at a reduced cost. Security has been the biggest concern among enterprises that are considering using the public cloud. For many organizations, the idea of storing data or running applications on infrastructure that they do not manage seems inherently insecure.

Cloud applications uses large data centers and powerful servers that host web applications and services and being an internet based utility it provides various services over a network. Anyone with a suitable Internet connection and a standard Internet browser can access a cloud application. So, it is prone to network based attacks.

- In 2007, excluding smart phones, approximately ten million sensors and devices communicated over a network. Currently, an estimated five billion such devices are now connected— a number that will continue to dramatically climb over the next decade, although estimates vary from twenty-five billion or fifty billion by 2020 to one trillion devices by 2025. The explosion in the number of devices has not resulted in manufacturers paying much attention to security.
- A small-sample study in Hewlett- Packard found that 7 out of 10 tested devices— including a smart TV, home thermostat and connected door lock— had serious vulnerabilities that could be attacked. A 2014 study by Symantec found that a seventy-five USD scanner could capture private or sensitive information from exercise trackers and other wearable devices. No one wants to build security into their devices, because no one is going to pay more for a secure device (Navnita Nandakumar *et al*, 2017).
- The infrastructure supporting the digital economy is growing more complex. Companies increasingly run their computing systems on virtual machines, cloud services have become a standard business practice and personal mobile devices increasingly creep into the workplace. The message that everyone is hearing is 'IT everywhere'but despite the influx of technology, there is a significant lack of trained security experts. — and not just in the online world according to Mystique Ahamad, professor at the GTRI College of Computing. The problem is that 'IT everywhere'also requires the need to safeguard IT everywhere Navnita Nandakumar *et al (2017)*.
- Computing systems, information systems and control systems with interconnecting components are today embedded in computer networks. The increasing interconnections have become a key infrastructure in different fields of applications, where the information security of Computer Networks is constantly confronted with seriousness severity of challenges. Some of the major causes of these situations are that the current configurations of Computer Network security systems are typically deterministic, static and homogeneous. Thus time complexity for attackers' to identify specific targets while scanning through Computer Network for vulnerabilities and accessing essential information is abridged. This provide attackers a better platform to develop, launch and spread attacks, but defenders are always at disadvantages coming up with late reaction (Kumar, U.et al. 2019).
- Cyber-attacks on businesses is universal so it's not a question of *if* but *when one will* be attacked. For instance If one is running a distribution or transportation business, one can fall victim to a cyber-attack. One possibility is the random defaced and this will cost temporary embarrassment or reputational damage to the Company. An attack could result in the theft of the company or employee credit card information. Cyber-attacks are a growing concern for businesses, and now's is the right time to take steps to foil the menace. Cyber criminals or hackers have gone sophisticated and can hide their digital tracks. Adware and spyware become the tools of choice as it becomes clear that data, and in particular actionable data, is worth billions.
- Security is fundamentally about protecting assets. Assets may be tangible items, such as a Web page or customer database or they may be less tangible, such as company's reputation.
- A guaranteed security service will augment the business performance of the service provider. A distributed system like Cloud can be protected by protecting the data,

making sure data is available for the customers, delivering high performance for the customers, using Intrusion Detection System to monitor every malicious activity. The service provider should have a support system for the clients in order that each client must be able to recover their data failure in cloud environment. The providers must make certain abstraction that the client does not face any problem such as data loss or data theft. Hence, encryption can be used to ensure reliability and authentication of data in the Cloud environment.

- As devices, systems and appliances increasingly communicate, verifying trust becomes a fundamental problem. Smart phones, which have become the mobile hub of people‘s lives, must have ways to determine how trustworthy, for example, a fitness band or a wireless speaker might be. Home routers or automation hubs will have to determine whether they trust a new security camera or an intelligent thermostat. While humans learn how to determine if another person or thing is trustworthy. In the digital world, trust is established through digital certificates, encryption and other information-security technologies.
- Encryption must be a key part of any distributed system security strategy. Not only that data should be encrypted while in storage service but it must also be encrypted during transit — when it may be most vulnerable to attacks.
- In Cloud Passage survey in 2017, respondents said that the two most effective cloud security technologies were data encryption (65 percent) and encryption of data in motion on networks (57 percent).

2. ENCRYPTION

Encryption is considered a best practice for any security-conscious organization. Encryption takes plaintext and encodes it into unreadable, scrambled text using mathematical algorithms, effectively rendering data unreadable unless a cryptographic key is applied to convert it. Encryption ensures data security and integrity, even if accessed by an unauthorized user, provided the encryption keys have not been compromised. Encryption can protect data in motion, referred to encryption in transit or encryption in flight, as well as at rest; meaning in storage. Encryption often occurs at multiple levels of a system, appropriate to the context of use and other system components. While encryption cannot protect against all cyber-attacks, the technology makes data theft a much more difficult task for hackers

2.1 Cryptography Strength.

Cryptography is an act of encryption it uses bijections functions(f) as the tool for encrypting messages and the inverse transformations (f -‘)are used to decrypt this ensure that only the intended recipient can read the message. An original piece of text (plaintext) is transformed into a concealed piece of text (ciphertext) and vice-versa.

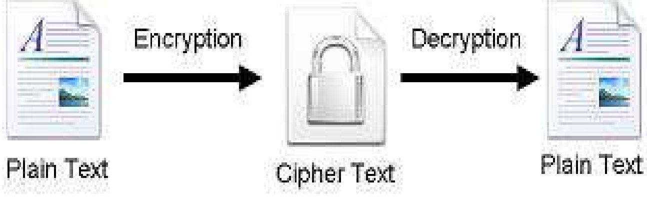

Figure 1 : Encryption System

- The basic idea behind cryptography is that a sender conceals (encrypts) a message using a mathematical algorithm (cipher) and a secret. A recipient that knows the cipher and secret can reveal (decrypt) the original message. Thus legitimate parties can transform plaintext to ciphertext and ciphertext to plaintext.
- A third party (the adversary), who has no knowledge of the secret key cannot have access to the plaintext.
- Cryptology: This is the scientific study of cryptography and cryptanalysis.
- Cryptanalysis: This is the process of deriving the plaintext from the ciphertext (breaking a code) without being in possession of the key or the system (code breaking)- using bruteforce.
- According to *The American Heritage College Dictionary*, 1987: The word "cryptology" is derived from the Greek ***kryptos*** (hidden) and ***logos*** (word).
- Cryptographic algorithm strength is determined by amount of computations an adversary needs to perform to recover the secret key and this is commonly referred to as the computational complexity of the cipher and the required space is called Key space.
- The Computational complexity of cryptography algorithm is deterministic and it is defines by the minimal number of bit-wise operations in terms of hardware gates (transistors) that are required to assemble a chip which can perform the complete cryptographic computation.

2.2 Cryptosystem:

There are two types of Cryptosystems: Asymmetric and Symmetric Cryptosystems. Symmetric cryptosystem also refers as private key cryptosystem uses only one key for both encryption and decryption of the data. Only those who are authorized to encrypt/decrypt would know the private Key. The encrypted messages are transmit over without any public keys attached to it. Whereas there are two different keys used for the encryption and decryption of data in Asymmetric cryptosystem (or public key cryptosystem). Public key is used to encrypt and the recipient uses his private key to decrypt. The keys are generated in such a way that it is impossible to derive the private key from the public key.

- The transmitter and the receiver both have two keys in an asymmetric system. However, the private key is kept private and not sent over with the message to the receiver, although the public key is.
- Symmetric could be Stream Cipher like RC4, SALSA, SOSEMANUK, PANAMA or Block Cipher like Triple DES and AES (Advance Encryption Standard). Stream Cipher encrypt/decrypt 1 bit or byte at once. While Block Cipher encrypt/decrypt a Block at once. A block is 64 bits or its multiple and therefore faster. Symmetric encryption algorithm perform invertible iterative Substitution- Permutation on plaintext to covert it Cipher text. The inverse function reverse Cipher text to plaintext at the other end.
- Asymmetric(Public Key Cryptography) is hard problem is mathematical problem such as integer factorization (RSA) or Discrete Logarithm Problem(ECC or HECC) that their inverse function seem infeasible.
- While Symmetric Cryptography offered good security for data, Key management and Authentication is a serious challenge. For 10 people/devices to communicate and exchange information, it will require (n*n-1)/2 keys for symmetric i.e. 45 keys whereas 10 keys is needed in Public Key Cryptography. In addition Public Key Infrastructure offer Digital Signature.

Public Key is used for encryption and signature verification while private key is used for decryption and signature generation. The two components required to encrypt data are an algorithm and a key. The algorithm generally known, and the key is kept secret. The key is a very large number that should be impossible to guess, and of a size that makes exhaustive search impractical. Symmetric cryptosystem uses the same key for encryption and decryption while asymmetric cryptosystem uses different key for decryption and encryption.

2.2 How to break a password or a key, in cryptography

Cryptography is all about counting techniques and probabilities. If a company's security policy states that a password should have four lowercase Letters followed by four numbers, in that order. There are 26 lower-case letters and 10 possible numbers, 0 to 9. The password space is 26. 26. 26. 26. 10. 10. 10. 10 = 4,569,760,000. If another company, decide to use eight upper-case letters, lower case letters, or numbers, in any order. So for each entry there are 26 + 26 + 10 possibilities and the total password space is 62. 62. 62. 62. 62. 62. 62. 62 = 628, for a total of 8.39 x $10^{17.}$ In cryptography, this are normally defined in numbers of bits. If a block encryption algorithm has a key of 128 bits; then, there are only two choices, either a 1 or a 0. The total number of possibilities is 2. 2. 2. 2. 2. ... = 2128 = 3.40282 x 10^{38} The exhaustive procedure of trying all possibilities, one-by-one, is also called a brute force attack.

3. HYPER ELLIPTIC FUNCTION.

Hyper Elliptic Curve for Encrypting System(C: y2 + h(x)y = f(x)): Hyper elliptic curves are a special class of algebraic curves and can be viewed as generalizations of elliptic curves. There are hyper elliptic curves of every genus $g \geq 1$. A hyper elliptic curve of genus $g = 1$ is an elliptic curve (Genus is the number of Non-Intersecting simple closed curve that can be drawn on the surface without separating it).

- Elliptic curves have been comprehensively reviewed. It is a notable tool in many key areas of applications including coding theory (e.g., Driencourt and Michon (1987) and van der Geer (1991); pseudorandom number generation Kaliski (1987); number theory algorithms Goldwasser and Kilian(1986); and public-key cryptography Koblitz (1987}, Miller (1986), and Menezes (1993).
- Hyper elliptic curves were a key ingredient in Adleman and Huang's random polynomial time algorithm for primality proving L. Adleman and M. Huang (1992). Hyper elliptic curves have also been considered in the design of error-correcting codes D. Le Brigand(1991), in integer factorization algorithms H.W. Lenstra, J. Pila and C. Pomerance , and in public-key cryptography N. Koblitz, (1989).
- Hyper elliptic curves over finite fields of characteristic two are good for hardware Implementation while Odd Characteristic is noted to be doing well in Software implementation.
- Charlap and Robbins (1988) in their introduction to elliptic curves provided self-contained proofs of some of the basic theory relevant to Schoof's algorithm for counting the points on an elliptic curve over a finite field R. Schoof (1985) and Hyper elliptic curve cryptography and elliptic curve cryptography (ECC) are similar once the Jacobian of a hyper elliptic curve is an abelian group. The Jacobian is isomorphic to the group of points on an elliptic curve in which an arithmetic operation can be performed. In particular scalar multiplication (g^a = ag= g+g+g+... a –times). Thus if b = g^a then a= Log$_g$b

3.1 Hyper elliptic curve for Public Key Cryptography.

Public key cryptography systems are based on sound mathematical foundations that are designed to make the problem hard for an intruder to break into the system. The major approaches that since 1976 have withstood intruder attacks, are the discrete logarithm The University of Adelaide problem (as in D-H), and the integer factorization problem as in RSA. The growing area of lightweight devices, such as mobile cell phones, PDA's, palmtops, where memory, processing power, bandwidths are limited, are constrained in using public key cryptography systems, which are based on large key sizes. The larger key requires higher computation power. Elliptic Curve Cryptography (ECC) has low key size for the user, and hard exponential time challenge for an intruder to break into the system. An ECC of 160 bits key, offers the same security as RSA 1024 bits key, so lower computer power is required. The advantage of elliptic curve cryptosystems is the absence of subexponential time algorithms, for attack.

Hyperelliptic curves provide shorter key lengths than elliptic curves for the same level of security. However, hyper elliptic curves of genus g=4, or higher, do not have the same level of security, as genus 2 or 3 curves, where attacks of subexponential time algorithms have been.

The Jacobian on a hyper-elliptic curve is an Abelian group and as such it can serve as group for the discrete logarithm problem (DLP) Mumford, D(1984). Assuming there is an Abelian group G and g an element of G, the DLP on G entails finding the integer given two elements of G, namely g and g^a. Pollard's rho method is the most efficient way to solve DLP and if the Jacobian has n elements, then the running time is exponential in log (n).

- Security of hyper-elliptic curves cryptosystem proves to be reliable and no existing algorithms with sub-exponent complexity has successfully attacked it R. Schoof (1985).
- Hyper-elliptic curves cryptosystem can acquire the same security level with shorter operating parameters. For hyper-elliptic curves cryptosystem with genus of 3, if the basic finite field is 60 bits, the security level HECC is equivalent to that of ECC with 180 bits, and it is far more secure than RSA with 1024 bits. In HECC, a secure Jacobian group with large prime number order can be constructed on a relatively smaller basic field.

Table 1: Comparison of Symmetric Key, ECC and RSA/DH/DSA

Computationally Equivalent Key sizes		
Symmetric	ECC	RSA/DH/DSA
80	163	1024
128	283	3072
192	409	7680
256	571	15360

3.2 Cellular Automata with Hyperelliptic curve encryption

- The Cellular Automata (CA) is the dynamic fruition of a one-dimensional array into a grid, made up of cells, each having a formalized state (1 or 0); this development is subject to a rule which provides the next state of the current cell, based on its current state and its neighboring cells. The Cellular Automatas are part of the dynamic systems family, they change over time, progressively as the current status of the cell changes- Wolfram. S. (1983)
- CA is a one-dimensional array, where each cell indexed by *i,* at time *t,* has a state s which is 0 or 1. $s_{t+1}(i) = f(s_t(i-1), s_t(i), s_t(i+1))$
- In a transition, sequence to a defined rule, the state of cell *i* at time *t* +1 depend on the old state and the neighbouring cells statement.
- *CA* containing two states and a neighborhood of space equal to 3, has 2^3 configurations, each configuration is named as a rule governing the *CA*, and each possible configuration leads to a state, so all possible rules are equal to or 256 possible rules. Stephen Wolfram. (2002).
- In this propose new stream encryption approach, the pseudo-random number generator is based on the use of Jacobians which Equivalent classes generated randomly from an Hyperelliptic curve, and their mapping in a grid constructed by the transitions of an elementary cellular automata

3.3 Threats, Vulnerabilities, and Attacks Defined

A threat is any potential occurrence, malicious or otherwise, that could harm an asset. In other words, a threat is any bad thing that can happen to the assets.

- Vulnerability is a weakness that makes a threat possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques. Weak input validation is an example of an application layer vulnerability, which can result in input attacks.
- An attack is an action that exploits vulnerability or enacts a threat. Examples of attacks include sending malicious input to an application or flooding a network in an attempt to deny service.
- To summarize, a threat is a potential event that can adversely affect an asset, whereas a successful attack exploits vulnerabilities in the system.
- To build secured applications, an holistic approach to application security is required and security must be applied at all layers. A secure application relies upon a secure network infrastructure. The network infrastructure consists of routers, firewalls, and switches.

3.4 Building Blocks of Security offered by Cryptography.

The division of information security into below logical components makes it easier to understand and deployed:

1. Authentication: Who you are. SSL uses Asymmetric Encryption. Web server hold private Key which can be compared if bind with requester Public Key in Digital Certificate.
2. Authorization: What you can do. Authentication is necessary for authorization. Role-based access control (RBAC) map security management to an organization structures.
3. Confidentiality: Data in transit not available to third party; using encryption. Only holder of private key can access.

4. Integrity: Tampering will be detected. By calculating the message digests using Hashing Algorithm e.g SHA-1.
5. Non-Repudiation: Public Key is bound to the identity of the owner. CA mapped Public Key with Digital Signature.
6. Availability: Certificate revocation list is used to manage Denial of Service attack. The Certificate of any suspicious Public Key is revoked and maintained in Certificate revocation list(CRl)

4. CORE SECURITY PRINCIPLES IN DISTRIBUTED SYSTEM:

- Compartmentalize: This can be achieved by restricting the potential damage using, Firewall, least privileged accounts and least privileged code.
- Using least privilege: If an attacker should manage to compromise security and run code, using account with minimal privileges and access rights will significantly reduce its capabilities.
- Apply defense in depth: Defense in depth means not rely on a single layer of security, or to consider that one of the layers may be bypassed or compromised.
- Not to trust user input: The application's user input is the attacker's primary weapon when targeting an application. It is to assume all input is malicious until proven otherwise, and apply a defense in depth strategy to input validation, taking particular precautions to make sure that input is validated whenever a trust boundary in the application is crossed.
- Fail securely: If an application fails, it should not leave sensitive data accessible but to return friendly errors to end users that will not expose internal system details, including details that may help an attacker exploit vulnerabilities in an application.
- Secure the weakest link: Any weak link chain in the host, Network layer or the application is an opportunity for breached security.
- Create secure defaults: The default account should be set up with least privilege and default account should be disabled by default and explicitly enabled when required
- Reduce the attack surface: By disabling or removing unused services, protocols and functionality the surface area of attack can be reduced.

4.1 Research Gaps

The explosion in the number of Micro-controller embedded devices has not resulted in manufacturers paying much attention to security. In 2007, excluding smartphones, approximately ten million sensors and devices communicated over a network. Currently, an estimated five billion such devices are now connected— the number will continue to increase dramatically over the next decade with an estimation of within twenty-five billion to fifty billion by 2020 and to one trillion devices by year 2025. Meanwhile Hackers uses IoT devices as springboards into corporate networks.‖ Their access points multiply as the number of devices used in the network increases and the more the genuine people connected on the network become more susceptible to hacking and other nefarious activities. Also, the Micro-controller embedded devices have restricted power and memory which a serious disadvantages to encryption based on integer factorizations like RSA and Tripple DSA as solution to them required high power and memory space. It is time to consider a more harder and chaotic problem that solution is not only feasible but also efficiently manage memory, Bandwidth and processor for Cryptography. The proposed encryption model based on Hyper-elliptic and Cellular automata uses less key and offer high randomness.

4.1 Research Questions

i. What are the weaknesses of the current algorithms and Cryptographic techniques in used in Distributed System and how do Secret Key transferred in a secured manner?

ii. What time does it take to generate a key pair (a private key and a corresponding public key) in Cloud Security System?

iii. How do we design a much more secured identity and session management mechanisms in Cloud Computing?

4.3 Research Aim And Objectives

The aim of the research is to Design and Implement an Adaptive and scalable encrypting System Solution in a distributed system using combination of strength of Hyper elliptic Cryptography and Cellular automata.

- The specific objectives of the research are:

1. To evaluate how encryption and decryption can take place much faster and better, without any loss of data security and at the same time guarantee Data protections and privacy across Devices.
2. To combined hardness of hyper elliptic function with chaotic nature of Cellular automata to build a strong and better encryption system that provide Security of Data at all Times and maintains Data Integrity in a Distributed System.

4.4 Significance Of Study

As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker. Security and privacy both are concerns in cloud computing due to the nature of such computing approach (Bisong & Rahman, 2011). The approach by which cloud computing is done has made it prone to both information security and network security issues (Rakhmi, Sahoo & Mehfuz, 2013; Qaisar & Khawaja, 2012).

- While Cloud computing brought ease of doing business it is equally a lucrative option to the attackers but the enormous possibilities of cloud computing cannot be disregarded solely for the security issues reason – the current temple of investigation and research for robust, consistent and integrated security models for cloud computing could only be the path of motivation.

4.5 Research Methodology

The researcher aimed at applying the following research methodologies: -

- To review the existing literatures on techniques and algorithms used in Public Key Encryption for Cloud Computing based System with a view of identify their inadequacies
- The study will survey the economic damages resulting from ethical hacking, Bluetooth hacking, Web permitting, Code injection and SQL injection in some selected corporate organization.
- The strength of Jacobian points of Hyper-elliptic curve and Cellular automata with opportunities to provide several randomness will be exploited in order to design a Scalable encryption system.

5. EXPECTED CONTRIBUTION TO KNOWLEDGE.

The expected contributions from this research outcome are as follows:

- It will promote Integrity, Authentication and Confidentiality of Cloud Computing based transactions which are the main requirements among the users.
- The intended final outcome of the research will model treats and address the inadequacies of the current Public Key algorithm used in Cloud based Computing and offer more resistant to hackers.
- It will design stronger encryption system algorithm using hyper elliptic function to address the current inadequacies in Data security tools use in Cloud Computing.
- It will also recommend more tightening administrative security measures to guide users and corporate organizations against emerging security treats to Distributed System.

6. CONCLUSION

Encryption technology must continue to evolve as hackers continue to become more savvy and sophisticated. Concerted effort must continue in research on different exciting technological advances in the encryption field, such as Hyper-Elliptic Curve Cryptography (HECC), homomorphic encryption, and quantum computation. Cryptography takes too much CPU time; the two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency at doing it. HECC with Cellular automata is a method of cryptography that allows encryption and decryption to take place much faster, without any loss of data security while Homomorphic encryption system allows calculations on encrypted data without decrypting it. Thus allow encryption across distributed systems, and ensure greater privacy for users- A financial institution could make assessments for individuals without revealing personal information.

The average case hardness of problems is the core for proofs-of-security for cryptographic schemes. The two established schemes for public-key cryptography are schemes based on the hardness of factoring and related problems and schemes based on the hardness of the discrete logarithm and related problems. Meanwhile both factoring and the discrete logarithm are known to be solvable in polynomial time on a quantum computers and algorithms for factorization tend to yield algorithms for discrete logarithm. Hence the to consider HECC with Cellular automata for public-key post-quantum cryptography.

REFERENCE:

1. Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006
2. Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS),257-259.
3. Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–.doi:10.1016/j.future.2011.08.009
4. Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences,2(10), 546-552.
5. *Thangasamy, Veeraiyah (2017). "Journal of Applied Technology and Innovation" (PDF). 1: 97*Web Services and Service Oriented Architectures, the Savvy Managers Guide, San Francisco, Calif: Morgan Kaufmann: Elsevier Science. ISBN: 1-55860-906-7
6. *Jun Tang, Yong Cui (2016). "Ensuring Security and Privacy Preservation for Cloud Data Services" (PDF). ACM Computing Surveys. 49: 1–39. doi:10.1145/2906153.*
7. *"What is a CASB (Cloud Access Security Broker)?". CipherCloud. Retrieved 2018-08-30.*
8. *"Identity Management in the Cloud". Information Week. 2013-10-25. Retrieved 2013-06*-Network Security: The Complete Reference. Emeryville, California: McGraw hill/Osborne. ISBN: 0-07-222697-8
9.]Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.
10. *"Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02. Retrieved 2010-01-25.*
11. *"Top Threats to Cloud Computing v1.0" (PDF). Cloud Security Alliance. Retrieved 2014-10-20.*
12. N. Koblitz, “Hyperelliptic cryptosystems”, Journal of Cryptology, 1 (1989), 139-150.
13. H.W. Lenstra, “Factoring integers with elliptic curves”, Annals of Mathematics, 126 (1987), 649-673.
14. Mumford, D. Tata Lectures on Theta. II. Boston, MA: Birkhuser, 1984.
15. R. Schoof, ―Elliptic Curves over Finite Fields and the Computation of Square Roots mod p‖, Mathematics of Computation, Vol. 44, No. 170, pp. 483-494, April 1985.
16. http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf
17. Wolfram. S. (1983). *Statistical mechanics of cellular automata*. *Reviews of modern physics*.
18. John Von Neumann. (1987). *The World of Physics: A small library of the literature of Physics from antiquity to the present,* The General and Logical Theory of Automata, New York.
19. Stephen Wolfram. (2002). *A new kind of science*. Wolfram Media.

20. Kumar, U.et al. Analysis of Network Security Issue and Its Attack and Defence. [online]. In: International Journal of Computer Science and Information Technologies, Vol. 7 (3), 2016, pp. 1029-1031. [accesat 14.03.2019]. availableat:https://www.researchgate.net/publication/301802858