Grenze International Journal of Engineering and Technology, July 2018

A Survey on Classical and Quantum Cryptography

Rohini S. H[1], Nikhita M[2], Pooja A[3], Jyoti H[4], Suma S[5] and Rajashekar B.Shettar[6]
[1-6]Dept. of E&C, B.V.B.C.T, Hubli, Karnataka India
[2-5]Dept. of E&C, K.L.E.T.U, Karnataka, India
{ Rohini H,Rajashekar.Shettar, rohini_sh,raj}@bvb.edu
{Nikhita M,Pooja A, nikhitamatti,242pooja, jyotihirekumbi369,sumashindhe10}@gmail.com

***Abstract*—Conventionally, every individual's personal data is been digitalized but as the digital theft could arise from hackers residing anywhere in the world, there is a need of huge improvement towards the security of an electronic data. Nowadays, in order to make the existing security system more robust and secure the research work is abundantly increasing day by day. The extra data/information we share which is confidential, greater is the risk of us falling to a data/information breach that is intentionally or unintentionally sharing of personal details to the unauthorized third parties. Now the hackers being intelligent and able to crack the currently available encryption methods, hence the scope for building uncrackable codes is more. This paper tries to summarize the view of top cybercrimes and different assets of Classical, Quantum and Post quantum cryptography to magnify the security of existing system.**

***Index Terms*— Digital, security, cyber crimes, cryptography, quantum.**

I. INTRODUCTION

In this era, security is one of the main constraints to concentrate on since the huge amount of data is been transmitted over the networks such as banks, telecoms, insurance companies, credit card issuers, mobile wallets, ecommerce companies, hospitals, and gas agencies etc. The attackers will steal most of the confidential information from these networks. The digital world is protected by encryption. Concept of encryption is that it's irreversible but not totally secure. For instance, banks started with 40-bit encryption 20 years back. That can be hacked in 5 minutes today. Now banks use 128-bit or 256 bit encryption. Presently, an unique identification number uses 2048-bit encryption [1]. Today it will take thousands of hours to break it, but not a decade from now. So before transmission of the data, sender must be aware of securing it by using some of the encryption techniques. Cryptography is a method which secures and authenticates the transmission of information over unsafe channels.

A. Top Cybercrimes

Lack of security motivates to make hack-proof, block chain system and resistant to quantum threats which is resultant of evolution of quantum technology [1]. The password is a secret key, known by both the server and therefore the user, making it possible to prove to the server that the identity provided is authentic[2].The hacking of those passwords is one of the targets of attackers through different means, the cybercrimes are increasing day by day. Safeguarding the systems to prevent cyber crimes at higher rates could be attained by

Grenze ID: 01.GIJET.4.2.510

two ways either by increasing the complexity of current systems or owing to the new technologies based on quantum aspects which would be the most difficult for frauds to hack the secrecy. The key issues in the secrecy of databases are accessibility, originality, integrity, confidentiality. The main targets of attackers are employment, birth, contact, and financial details where in they can easily have the access over user's financial accounts. Though the protection system is rising strictly, meantime the crimes are also increasing statistically. Following are the top cybercrimes:

ATM theft: The attackers/fraudsters/hackers target to rob the plenty of money through automated teller machines using ATM card holder's details.
Fake processing unit: It is an unit where a cable is connected to the network machine. The attacker detaches the ATM machine from bank's network and then connects a device that act as a fake processing unit. The processing unit is used to handle the trays of cash and send orders to the ATM, requesting money from the chosen tray of cashes. It's easy as the hacker/attacker can now use any card or input any pin code and theft transaction looks legal.
Keypad Overlays: An ATM keypad overlay is essentially a dummy keypad that's placed over the existing ATM keypad. An overlay will record and capture card holder's secret PIN number that he/she enter when taking money from an ATM machine [3].
Skimming: The secret electronics is been fixed in ATM's to steal personal information on user's card and record pin number to access all money directly from the ATM's.
Hidden Cameras: It looks like a flyer holder and is fixed in a position to observe ATM PIN entries and the attackers steal the card details and utilize the PIN numbers to withdraw money from many accounts [4].

Biometric theft: Presently, systems of Government sectors, Hospitals, colleges are usually fixed up with the biometric machines where in the finger prints, face recognition, iris recognition of each individual is been taken for a unique identification. The attackers/hackers hack the personal data of the public.
Processing and transmission level attack: Many of the biometric identifiers transfer test data/information to local or remote work stations for further processing. Thus it is a vital importance that this communication should be reliable and secure. Most of the biometric identifiers convert information/data into a code, however not all applications and tools give themselves to encryption.
Spoofing attack: It is a scenario in which one individual or program successfully masquerades as another by falsifying data, there by acquiring an illegal accessibility. Many of the protocols in IP/TCP suit do not provide mechanism for authenticating the source or destination of a message. In particular, in the middle attacks IP and ARP spoofing may be used to leverage man against host on a computer system.
Input level attack: At the point of test acquisition and initial processing Vulnerabilities are spoofing, bypassing and also problematic vulnerability is overloading. To prevent system by harming output device or overwhelming it in the attempt to generate errors also called Buffer overflow attack which is known as overloading.
Back end attack: The hacker can seize the authentic details of authorized individual by the method of introducing templates right away in to the storage database without following any appropriate procedure, this is one of the apparent type of back end attack. This mainly includes matching or decision subsystems, or a combination of both attacks.

Net banking: As the net banking is frequent in use by the citizens to carry out the transactions, which is much advantageous for the attackers to hack the accounts through different tricks as their target is to steal the money.
Following are the different attacks on accounts:
Phishing: This is the technique used to hack login details and passwords of users from the websites. Phish pages are simply fake pages that look like original page where user feel that it is a legally certified website but without any clue to him/her, the confidential information will be directly hacked by the attackers sitting elsewhere in the world.
SMS Spoofing: This is the new technology in which a user receives a SMS message on his/her mobile phone which feels to be coming from a legal bank but this is the threat that fools the user to steal the money from his\her accounts.
Malware: This is a harmful software program that accesses and alters the computer system without any idea to the user or owner that he is been hacked by the Malwares such as viruses, Trojan horses, worms, etc. [6].

Shopping cards: Phishing site and instant messenger are the two modes which are used to spread and inject the malware by shopping malls. Both methods are very effective because attackers know the expectation of the user.
Phishing Site: As explained previously in net banking the same attack is seen through the shopping website.
Instant messenger: It is one of the most highly used modes for injecting malware. Attracting the public in terms of screening discount news in shopping groups which is nothing but dispatching the malware to a file. Once the user executes the malware, the major thing that the malware will do is monitoring of the browser. Immediately, when it found the user is at a payment page, the malware will change the request and the user's payment will actually go to frauders/attacker's bank account [7].

B. Reasons for growing cyber crimes [1]

- Increased use of emerging tech
- Lack of security culture
- Leakage of sensitive information
- Lack of user awareness
- Increased exposure to internet

Thus these are the top cyber crimes, and now let us see how these attacks can be prevented using different security tricks.

II. Classical Cryptography

In this era of use computer's technology to reserve, recover, transfer, and change information, often in the context of a business, banks or any other enterprise the need for secrecy has achieved huge importance. As most of our sensitive and confidential information is stored in computers. The necessity of data protection becomes progressively important. Cryptography is one of the best methods of protecting sensitive data from being stolen by unwanted third parties. It is important to design techniques and solving methods that offer a fixed, genuine, strong and experimental transmission. The most popular and essential technique for secure communications is the Cryptography: the art of keeping secret of confidential message information and making it such that it will not be understood by any unauthorized party. Cryptography is required to transfer personal or confidential data over the network channel. It is also demanding in wide range of applications which involves applications of mobile and networking. Cryptographic algorithms play an important role in providing the data security against harmful attacks. The two main attributes which determine and discriminate one coding algorithm from another are its capability to reliably secure the protected information/data against harmful attacks and its speed and potency in doing so.

Algorithms*:* The fundamental set of cryptographic algorithms can be divided into three groups:

1. Symmetric
2. Asymmetric
3. Hash functions

III. Quantum Technology

Quantum technology is comparatively a new and very knowledge based field of research and development. . We are currently in the middle of a second quantum revolution. The primary quantum revolution gave us new set of rules that govern physical actuality. To build new technologies, the secondary quantum revolution will take these new rules. It is a new field of physics and engineering, that transitions number of the properties of quantum physics particularly quantum entanglement, quantum superposition and quantum tunneling, into experimental applications such as quantum- computing, sensing, cryptography, simulation, metrology and imaging. Quantum technology allows us to assemble and handle the elements of a complex system governed by the laws of physical science.

Quantum cryptography: It is popular that quantum computers can solve certain problems which are unmanageable for classical computers; for example, Shor's algorithm, and Grover's algorithm and more recently Harrow, Hassidim and Lloyd's algorithm for systems of linear equations. In current years, governments and industries around the world have been racing to build quantum computers. As occurred in the history of classical computing, once quantum computers are commercialized, programmers will certainly

need a modern platform that can express and implement quantum algorithms without considering the trivialities of their circuits. Such a platform will be even more helpful for quantum programming than in classical computing because physically implement quantum algorithms in a quantum system is somewhat counterintuitive[9]. It is not a new procedure to encrypt and decrypt data. Instead it is a method of using photons to generate a cryptographic secret key and transmit it to a receiver using a suitable transmission channel. A cryptographic key plays the most important role in cryptography; it is used to encrypt/decrypt data. Quantum cryptography is the only known method for transmitting a secret and confidential key over distance that is secure and reliable in principle and based on the laws of physics. Existing methods for transmitting secret keys are all based on unproven mathematical assumptions. These same methods also are at risk of being cracked in the future using certain set of algorithms.

The central phenomena of quantum technology: The main aim of quantum technology is to deliver useful tools and actions that are based on circumstances of quantum physics which involves:

1. Superposition
2. Heisenberg's Uncertainty Principle
3. Entanglement
4. Squeezed states
5. Decoherence

TABLE: I COMPARISON OF QUANTUM AND CLASSICAL CRYPTOGRAPHY

Properties	Quantum Cryptography	Classical Cryptography
Based on	Quantum Mechanics	Mathematical calculations
Growth	In the process of developing and fully not tested	Advanced and tested
Current Infrastructure	Sophisticated	Widely used
Digital Signature	Not existing	Existing
Bit rate	1Mbit/s average	Depends on computing potential
Cost	Crypto chip €100,000	Almost zero
Register storage(n bit)at any moment	One n bit string	2^n n-bit strings
Transmission range	10 miles max	Million of miles
Requirements	Hardware and transmission lines	Software and transferable
Life expectancy	No modify as based on physics laws	As computing power increases, there is need of change
Medium	Dependent	Independent

IV. POST QUANTUM CRYPTOGRAPHY

The main objective of quantum-resistant cryptography is to progress cryptographic models that are resistant against both quantum and classical computers, and can interoperate with current communications. Conventional computers are binary digital gadgets based on transistors. Quantum computers which are just different from super computers; they use quantum bits to store data/information as 0, 1 or even both at the same time. Thus the scope for new algorithms in post quantum cryptography which are resistant to quantum computations, as of now there are five proposals, which are under study the following are the different cryptographies:

1. Lattice
2. Multivariate
3. Hash
4. Code
5. Super singular elliptic curve isogeny cryptography[8]

V. CONCLUSION

Finally, the future is going to be networked worldwide. Hence safety of these networks is acquiring vast significance globally. Undoubtedly, Science and information Technology grows day by day. We need to concentrate and employ the advancements in emerging fields of Science and information Technology to come up with highly secured and reliable and robust in practices.

FUTURE SCOPE

The major objective of research effort on cryptography is to meet the need of maintaining the secrecy of confidential data by altering existing algorithms, building the key generation model, approach on new mathematical equations. The ability of easily hacking most confidential information should be prevented by improvising the complexity of existing systems using the emerging technologies of quantum physics.

ACKNOWLEDGMENT

The authors wish to thank, Head of the department, staff members, teaching and non - teaching staff for the successful completion of the paper.

REFERENCES

[1] https://economictimes.indiatimes.com/news/economy/policy/how-safe-is-digital-india-indias-vast-data-pools-need-to-be- secured-with-tighter-de-risking-tools/articleshow /62489823.cms
[2] http://theconversation.com/passwords-security-vulnerability-constraints-93164
[3] http://www.identitythefteaid.org/types-of-identity-theft/atm-overlay/
[4] https://www.snopes.com/fact-check/atm-camera/
[5] Rubal Jain and Chander Kant, "Attacks on Biometric Systems: An Overview", International Journal of Advances in Scientific Research 2015; 1(07): 283-288
[6] Zarka Zahoor,Moin Ud-din and Karuna Sunami "Challenges in Privacy and Security in Banking Sector and Related Countermeasures", International Journal of Computer Applications (0975 – 8887) June 2016 Volume 144 – No.3
[7] https://www.virusbulletin.com/uploads/pdf/conference_slides/2012/Lu-VB2012.pdf
[8] https://access.redhat.com/blogs/766093/posts/3031361
[9] Shusen Liu,. Xin Wang, Li Zhou, Ji Guan, Yinan Li,Yang He, Runyao Duan,† and Mingsheng Ying "A Quantum Programming Environment", Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia
[10] Abdulmonam Omar Alaswad, Ahlal H. Montaser, Fawzia Elhashmi Mohamad "Vulnerabilities of biometric authentication Threats and countermeasures", International Journal of Information & Computation Technology,ISSN 0974-2239 Volume 4, Number 10 (2014), pp. 947-958
[11] Aakash Goyal, Sapna Aggarwal and Aanchal Jain ,"Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper", 5th IEEE International Conference on Advanced Computing & Communication Technologies ICACCT-2011 ISBN 81-87885-03-3
[12] David R. Kohel, "Cryptography",Creative Commons Attribution-Noncommercial-Share Alike 3.0 Unported License,August 4
[13] Berstein,D.J.:Buchmann,J.:Dahmen,E.(Eds.)"Post-Quantum Cryptography",2009.X,246 p.,Hardcover ISBN:978-3-540-88701-0
[14] Jung-Shian li, Ching-Fang Yang, 2009. "Quantum Communication in Distributed Wireless Sensor Networks": IEEE 2009.
[15] Minakshi Bhatt , Anjali Aneja , Sonam Tripathi , Classical Cryptography v/s Quantum Cryptography A Comparative Study, International Journal of Electronics and Computer Science Engineering, ISSN- 2277-1956
[16] T.M.T. Nguyen, M. A. Sfaxi, S. Ghemaouti-Helie, 2006. "Integration of Quantum Cryptography" in 802.11 Networks: in Proc. 1st Int. conf. on Availability , Reliability and Security.
[17] Rivest R., ShamirA., and Adleman L., "On digital Signature and public key Cryptosystems", MIT Labs for computer science, Technical Report, MIT/LCS/TR-212(January)