ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Study on 4pioneering Technologies Imminent With Cybersecurity

M.Anitha Priyadharshini, S.Nivedha

Assistant Professor, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India

PG Scholar, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India

ABSTRACT: Cyber security states the body of technologies, practices, and processes intended to protect networks, devices, programs, and data from attack, damage or unauthorized access. Cyber security has come a long way over the decades, but hackers and cyber security experts are constantly trying to one-up each other in terms of technological sophistication and preparedness. Every time we take a major step forward in terms of reliable security, cyber criminals are there to match us. Even so, we can always make forward progress toward building something more reliable-there's always room for improvement in our existing systems, and new technologies on the horizon. This paper provides the analysis of different technologies that pave the future of cyber security.

KEYWORDS:Quantum key distribution, Blockchain technology, Biometrics and Dust.

I. INTRODUCTION

Cyber security is the state of being protected against the criminal or unauthorized access of electronic data. Accordingly, there will never be an "unhackable" device or piece of software; there will always be vulnerabilities in any system you have in place. Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organization transmit sensitive data across networks and to other devices in the course of doing business, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. The following are the most promising technologies coming to keep our digital information and communications safer.

- Quantum Key Distribution
- Blockchain Technology
- Biometrics
- Dust

II. QUANTUM KEY DISTRIBUTION

It sounds like some kind of super power, but as WIRED writes, quantum key distribution could be the future of encryption technology. Quantum physics involves the study of subatomic particles, which behaves strangely, against out intuitions on small scales. We're already using the quantum computers, which take advantage of particles that can exist in two states at the same time(as a particle in a wave).quantum entanglement involves two particles that affect each other's position, even at a distance. Conventional encryption involves a lock-and-key method of creating and then cracking a code – but these can be easily copied and cracked. Quantum key distribution relies on quantum entangled particles that are virtually uncopiable and tremendously hard to crack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Quantum Key Distribution (QKD) was first introduced in 1984 by Bennett and Brassard, it is a method for distributing a secret key between two parties. Due to a fundamental property of quantum physics known as the no-cloning theorem, any attempt made by a third party to eavesdrop inevitably leads to errors that can be detected by the sender and receiver. Modern QKD systems conventionally use a qubit system for encoding information, such as the polarization of a photon. QKD systems often rely on polarization of light for encoding, thuslimiting the amount of information that can be sent per photon and placing tight bounds on the error rates that such a system can tolerate. Such systems are applied with no trouble because technology for encoding and decoding information in a qubit state-space is graciously available today, enabling system clock rates in the GHz regime.

A. *Quantum Key Distribution Protocols*

They are used in quantum key distribution. The first protocol of that kind was BB84, introduced in 1984. After that, many other protocols have been defined.

- BB84
- Decoy state protocol: A practical QKD scheme using imperfect single photon sources, such as weak coherent state sources
- E91 protocol: entanglement protocol
- MSZ96 protocol
- SARG04
- COW protocol: coherent one way protocol by Gisin
- DPS protocol: differential phase shift by Yamamoto
- KMB09 protocol: High Error-rate QKD protocol by Khan et al.
- S09 protocol: Protocol with Private-Public Key arXiv
- S13 protocol: Quantum Key Distribution From A Random Seed arXiv

B. *QKD Networks*

- SECOQC

The world's first computer network protected by quantum key distribution was implemented in October 2008, at a scientific conference in Vienna. The name of this network is SECOQC (Secure Communication Based on Quantum Cryptography) and EU funded this project. The network used 200 km of standard fibre optic cable to interconnect six locations across Vienna and the town of St Poelten located 69 km to the west. One of the main objectives of SECOQC was to bring about a significant advance of the enabling QKD technology. The realization of this objective culminated in a major dedicated effort of developing highly mature QKD link devices for the SECOQC network prototype. It was decided to include a wide range of different QKD implementations, while imposing a set of stringent requirements.

1. Plug & play
2. One-way weak coherent pulse qkd, phase coding
3. Coherent one-way (cow) system, time coding
4. Entanglement-based (ent) qkd
5. CV qkd with coherent states
6. Free-space (fs) qkd

- Swiss Quantum

Id Quantique has effectively completed the longest running project for testing Quantum Key Distribution (QKD) in a field environment. The main goal of the Swiss Quantum network project installed in the Geneva metropolitan area

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

in March 2009, was to validate the reliability and robustness of QKD in continuous operation over a long time period in a field environment. The quantum layer operated for nearly 2 years until the project was shut down in January 2011 shortly after the initially planned duration of the test.

- Los Alamos National Laboratory

A hub-and-spoke network has been operated by Los Alamos National Laboratory since 2011. All messages are routed via the hub. The system equips each node in the network with quantum transmitters i.e., lasers, but not with expensive and bulky photon detectors. Only the hub receives quantum messages. To transfer, each node sends a one-time pad to the hub, which it then practices to interconnect securely over a classical link. The hub can route this message to another node using another one time pad from the second node. The entire network is secure only if the central hub is secure. Individual nodes require little more than a laser. Prototype nodes are around the size of a box of matches.

III. BLOCK CHAIN TECHNOLOGY

A blockchain is an electronic ledger of digital records, events, or transactions that are cryptographically hashed, authenticated, and maintained through a “distributed” or “shared” network of participants using a group consensus protocol. Blockchain is a term associated with the technology of Bitcoin. Blockchain is a system of collaborative information storage, exchange, and retrieval that maintains a public record of ownership. It’s how bitcoin transactions are able to take place, and remain consistent, without any single institution defining or monitoring those transactions, and without any outside interference to commit digital theft. Shaping tomorrow predicts that within a few years, most major banks as well as other financial-related companies like insurance institutions will be using blockchain to greater secure their financial transactions. Blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world.

The blockchain distributed ledger technology for business transactions seems to be more viable and growing acceptance. For example, new cryptographic ledger approaches use blockchains to execute simple tasks of verifying contracts. The main proposition is that the blockchain establishes a system of creating a distributed consensus in the digital online world. It opens the door for developing a democratic open and scalable digital economy from a centralized one. Thus, “the blockchain, a means to accurately tracking any form of transaction, has significant value beyond the realm of monetary transfer.” The potential range of the blockchain utility spans intellectual property, market security, and internet of anything.

The “blockchain technology is best described as a concept that involves a number of key components including (but not limited to) validation, a consensus mechanism, replication, and storage.” These themes were consistent focus points codified from the subject matter expert interviews. Expanding on these key themes, important cryptographic ledger components include:

- Consensus Mechanism
- Smart Contract Execution
- Validation
- Peer-to-Peer Replication
- Storage
- Auditability
- Identity and Authentication
- Exception Handling
- Read and Write Permission
- Confidentiality and Privacy

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

IV. BIOMETRICS

Biometrics means "life measurement" is mainly used for identification and access control, or for identifying individuals that are under surveillance. It is the dimension and arithmetical analysis of people's physical and behavioural characteristics. The technology is the basic premise of verificationthat everyone is unique and an individual can be identified by his or her intrinsic physical or behavioural traits.For example, your phone may use a thumbprint scan before allowing you to access the data inside, or a device may scan your retina before permitting you access to a building. Since these personal identifiers are incredibly hard to mimic, especially remotely, they could greatly enhance security in a number of areas.There are two main types of biometric identifiers:

1. Physiological characteristics: The shape or composition of the body such as fingerprints, dna, face ,etc
2. Behavioral characteristics: The behavior of a person such as typing rhythm, gait, gestures and voice.

A. *Types of Biometrics*

- Dna Matching
- Ear
- Eyes - Iris Recognition
- Eyes - Retina Recognition
- Face Recognition
- Fingerprint Recognition
- Finger Geometry Recognition
- Gait
- Odour
- Typing Recognition
- Vein Recognition
- Speech Recognition
- Voice Recognition

V. DUST

DUST or Disintegration Upon Stress-Release Trigger, is a technology that allows electronic devices using full-performance microchips to be disintegrated on command, leaving only tiny fragments that are invisible to the human eye. Engineers at Xerox PARC have designed a prototype chip capable of self-destructing it is named DUST, or Disintegration Upon Stress-Release Trigger. The researchers at Xerox PARC believe that their integrated self-destruct chip could represent the ideal solution for the storage of high-sensitive data, including the encryption keys. The potential applications of the DUST self-destructing chip include remote sensing or battlefield communications kit andof course drones.

VI. CONCLUSION

It's hard to say when these developments might actually become main stream. Some of them sound like technology straight out of science fiction, but the reality is that scientists and engineers are already working on these futuristic solutions and probably some even more advanced technologies that's being kept from the headlines. Some of the biggest challenges include the cost of developing these technologies, which should improve over time, and convincingly demonstrating the reliability of these protocols. We could be as close as a few months away from their custom.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

ACKNOWLEDGENMENTS

Our sincere thanks to the experts supported this work and their valuable comments.

REFERENCES

1. Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Modern Phys.*
2. Extance, A. (2015). Bitcoin and Beyond. Nature. Macmillan Publishers Limited. October 1, 2015. Vol. 526,
3. Buterin, V. (2013). Bitcoin Network Shaken by Blockchain Fork. *Bitcoin Magazine*, 13 March. Retrieved from https://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/
4. Buterin, V. (2015a). *Visions, Part 1: The Value of Blockchain Technology*. Ethereum Blog. 23 April. Retrieved from https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/
5. Fung C-H F, Tamaki K, Qi B, Lo H-K and Ma X 2009 *Quant. Inf. Comput*
6. A. K. Jain, A. Ross, and S. Pankanti, \Biometrics: a tool for informationsecurity," IEEE Transactions on Information Forensics and Security
7. A. Jain, L. Hong, and S. Pankanti, \Biometric identi_cation," Commun. ACM.