Wesleyan Journal of Research, Vol.14 No.12 (April 2021)

ISSN : 0975-1386
Research Article (Technology)

A STUDY OF CRYPTOGRAPHY AND TECHNIQUES OF CRYPTOGRAPHY

[1]Dr.Santosh Madhusing Chavan, [2]Dr. Shyamsundar Ashokrao Aboj

[1]Assistant Professor Shri Shivaji College Akola, Sant Gadge baba Amravati University, Amravati.

[2]Assistant Professor, Lal Bhadur Shastri Sr. College, Parsur, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad.

E-mail: [1]santoshchavan0803@gmail.com, [2]shyamaboj786@gmail.com

Abstract — Security and privacy of information and communication have become very important aspects o
day's era, which is experiencing a burst of technological innovation like never before. The benefits
ptography and cryptanalysis can be found here. Cryptography ensures the integrity, availability, and identity
sers, as well as the confidentiality, authentication, and protection and privacy of data that can be given
m. We described and analysed symmetric cryptographic algorithms such as DES, Triple DES, Blowfish, AE
IDEA, as well as asymmetric key cryptographic algorithms such as RSA, in this paper. They were evaluat
erms of data security, key size, block size, and functionality. We've also dabbled in DNA cryptography, Ellipt
rves-based cryptography, and Quantum cryptography, all of which are newer trends in the field of cryptograp
, in our opinion, have enormous potential.

Keywords: Cryptography, Encryption, DES, RC5, Triple DES, AES, RSA, Quantum Cryptography, DNA Cryptograp

Article History

Received: 01/04/2021; Accepted: 08/04/2021

Corresponding author: Dr.Santosh Madhusing Chavan

I INTRODUCTION OF CRYPTOGRAPHY

Cryptography is the study of writing in secret code and is an ancient craft, the first documented use
cryptography in making dates back to about 1900 B.C., when an Egyptian recorder drew with non-stand
hieroglyphs. Cryptography came out of nowhere at some stage or another in the wake of making, with applicati
ranging from assuaging notes to war-time battle designs, according to many experts. It's not surprising that u
es of cryptography appeared not long after the improvement in PC communications, regardless of how y
dicate it. Cryptography is fundamental in data and telecommunications when dealing with any untrusted mediu

cials for all intents and purposes any structure, especially the Internet. There are some explicit security
within the context of any application-to-application communication, including Authentication. The path
implying one's character. (The fundamental sorts of host-to-have approval on the Internet today are
sed or address-based, the two of which are comprehensively slight.)

ity/Assurance: Ensuring that nobody can look at the message adjacent to the orchestrated gatherer
grity: Assuring the expert that the got message has not been changed at all from the first.
ervation: A section to demonstrate that the sender incredibly sent this message

ssion, cryptography had been developed to protect data from theft or alteration, as well as to be used for
verification. When in doubt, three types of cryptographic plans are consistently used to achieve these
ys: confuse key (or symmetric) cryptography, open key (or hitter kitter) cryptography, and hash works.
both are depicted below. The simple decoded information is indicated as plaintext in all cases.

ted into figure material, which will be decoded into accessible plaintext in this manner (for the most part)
ssing on gatherings would be proposed as Alice and Bob in a vital heap of the depictions beneath; this is
al wording in the crypto sector and writing to make it less perplexing to see the passing on gatherings
could be referred to as Carol and Dave if there is a third or fourth gathering to the correspondence. Eve is
eavesdropper, and Trent is a confided in outcast. Mallory is a pernicious get-together, Eve is an eavesdropper
ent is a confided in outcast.

II. STUDY OF CRYPTOGRAPHY

Types of Cryptography Algorithms

There are a few distinct procedures for dealing with cryptographic checks. For inspirations driving this pap
will be coordinated reliant on the proportion of keys that are used for encryption and unscrambling, whi
portrayed by their application and use. The three sorts of estimations that will be analysed are:

Public Key Cryptography (PKC): Uses one key for encryption and another for unscrambling
Secret Key Cryptography (SKC): Uses a solitary key for both encryption and unscrambling

A STUDY OF ROUTING PROTOCOL IN WIRELESS SENSOR NETWORK

Dr. Santosh Madhusing Chavan
Assistant Professor Shri Shivaji College Akola, Sant Gadge baba Amravati University, Amravati.
santoshchavan9881@gmail.com,

Dr. Shyamsundar Ashokrao Ahuj
Assistant Professor, Lal Bhadur Shastri Sr. College, Partur, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, shyamahuj786@gmail.com

Abstract: Wireless sensor network is emerging field because of its wide applications. It is a wireless network which subsist a group of small sensor nodes which communicate through radio interface. The four basic elements of these sensor nodes are sensing, computation, communication, and control. With the notion that there will be cases for energy awareness, many routing, power management, and data dissemination protocols have been explicitly developed for wireless sensor networks. However, the key resource constraints are limited energy, communication capability, storage, and bandwidth. The flexibility, fault tolerance, high sensing fidelity, low cost, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. Our survey is based on various aspects of routing protocols in wireless sensor networks.

Keywords: WSN, Sensor nodes, Routing, Ad hoc networks

I INTRODUCTION OF WSN

Wireless Sensor Networks (WSNs) have begun to draw the attention of researchers with the fast technical advancement of wireless technologies and embedded electronics. A standard WSN consists of small devices that are known as nodes. New technologies and standards are used for wireless sensor networks. They include lightweight, energy-efficient machines, co-design of hardware/software, and support for networking. Wireless sensor networks are now an integral part of everyday, technological and military systems of everyday life. As new technologies are evolving and new applications are being created, this is a fast-growing field. These nodes have a built-in CPU, some intelligent sensors and minimal processing power. Nodes are used with these sensors to track environmental conditions such as heat, humidity, vibration and noise surrounding them. In every WSN, a node usually includes a transceiver unit, a sensor controller, a computer unit, and a control unit. By having nodes capable of communicating with each other to relay data collected by their sensors, these units perform critical tasks. To have a centralised structure, coordination between the nodes is essential. The need for this device contributes to the growth of the notion of the internet of things (IoT).

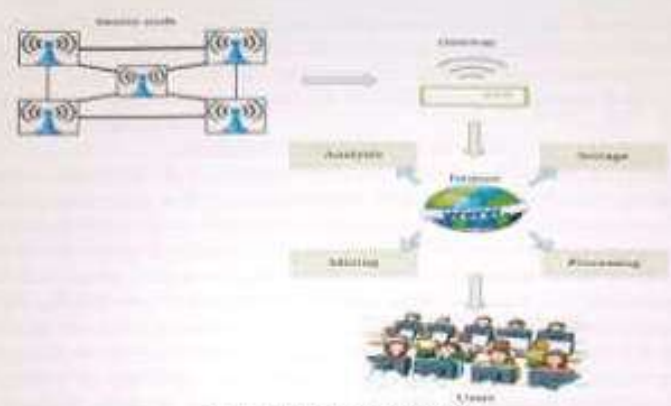

Figure 1: Architecture of WSN

A WSN may usually be described as a network of nodes that act in a cohesive way to sense and regulate the world around them. Through wireless networks, these nodes are linked. This relation is used by nodes to communicate with each other. There are 3 elements in the structure of a standard WSN such as sensor nodes, internet and user nodes. The sensor area constitutes sensor nodes and gateways. Gateways and observers are linked by special networks or, most often, through the internet

II. COMPONENTS OF WSN

A WSN consists of multiple sensor numbers and a gateway to offer an Internet connection. The components of WSNs are sketched in figure 9.

Figure 2 Components of WSN

Sensor Unit

A sensor node is a compact computer with a low power supply. While it has small energy capacity, it has a simultaneous processing rule and has a low price as well. Individual units of a sensor node accomplish data collection and data transfer steps. The power source is located at the base of the sensor node. It provides power for different sensor node devices, such as sensor units, radio and CPU.

Microcontroller

Usually, a microprocessor and a flash memory are made of the CPU of a sensor. It provides connectors for most sensor nodes that can easily add external processing units and sensors to the main device. For the critical functions of the CPU, decision-making and coping with collected data can be identified as examples.