Asian Journal of Research in Computer Science

12(3): 1-13, 2021; Article no.AJRCOS.74754
ISSN: 2581-8260

A Statistical Study into Network Security Issues of IT Companies in Accra

Abraham Tetteh [a*], Richard Essah [b], Afroj Jahan Badhon [b], Yaw Adjei Asante [c] and Amoa-Boateng Patrick [d]

[a] Bia Lamplighter College of Education, P.O.Box 97, Sefwi-Debiso, Ghana.
[b] University Chandigarh University, Punjab - 140413, India.
[c] Kwame Nkrumah University of Science and Technology, Ghana.
[d] University of Ghana, Legon P.O. Box 40, Ghana.

Authors' contributions

This work was carried out in collaboration among all authors. Author AT designed the study and wrote the first draft of the manuscript. Authors RE and AJB managed the analyses of the study. Authors YAA and ABP managed the literature searches. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v12i330282
Editor(s):
(1) Prof. G. Sudheer, GVP College of Engineering for Women, India.
Reviewers:
(1) Hamzah Hadi Qasim, Iraq University College, Iraq.
(2) Azahari Bin Salleh, Universiti Teknikal Malaysia Melaka, Malaysia.
(3) Bilal Khalil, Mayo Clinic, USA.
Complete Peer review History: https://www.sdiarticle4.com/review-history/74754

Original Research Article

Received 01 August 2021
Accepted 05 October 2021
Published 09 November 2021

ABSTRACT

Wireless Sensor Network (WSN) is a rising technology that offers a great assurance towards a variety of revolutionary applications such as military and public. As wireless sensor networks continue to develop, there is a high importance in security mechanisms. As sensor networks works with responsive data and operate in antagonistic environments, it is crucial to address the security issues. The sensing technology united with wireless communication and processing power makes it rewarding. Due to these computing and inherent constraints in resource, sensor network security has special challenges. The low cost and collaborative nature of the wireless networks (WNs) offers significant advantages upon the conventional communication techniques. The wireless communication technology has several kinds of security threats. The spotlight of this paper is towards addressing the security issues and challenges of WSNs. Here the idea is to identify the threats and security mechanism of wireless sensor networks among WSNs companies in Accra. This paper will contribute to the literature of Wireless sensor

**Corresponding author: E-mail: abrahamtetteh@blce.edu.gh;*

networks security issues and challenges in society especially in Ghana. It is concluded that wireless sensor networks have security impact and challenges on information security in IT companies in Accra.

Keywords: Wireless; sensor networks; IT companies; challenges and communication technology.

1. INTRODUCTION

Today Internet has turned out to be one of the essential pieces of our day by day life. It has changed how individuals live, work, play and learn. IOT systems as of now rely primarily on sensors and remote systems that allow remote access to data or application [1]. In any case, IOT offers noticeable assurance in the field of wellbeing mindfulness more than any other area. As a maxim goes "Wellbeing is riches" it is astoundingly pivotal to make use of the development for better prosperity. Subsequently an IOT system is added, which gives secure wellbeing mindfulness checking. The present patient screen frameworks in healing facilities permit persistent checking of patient imperative signs, which require the sensors to be hardwired to available, screens or PCs near the patient's bed, and limit the patient to the ward assigned by the doctor.

Indeed, even subsequent to associating these frameworks to a specific patient, a par prompt fiasco on account of a human blunder. Late years have seen a rising enthusiasm for wearable sensors and today a few gadgets are financially accessible for individual human services, fitness, and action mindfulness. In light of current mechanical patterns, one can promptly envision a period sooner rather than later when your routine physical examination is gone before by a two– three-day time of ceaseless physiological checking utilizing economical wearable sensors. Such a problematic innovation could transformatively affect worldwide medicinal services frameworks and radically lessen social insurance costs and enhance speed and exactness for analyze.

Wireless Sensor Networks (WSN) is an emerging technology involving distributed sensor nodes through multi-hop routing [2]. Wireless sensor networks gain rapid popularity due to tiny sensing devices. They are the potential low-cost solutions to environmental monitoring, surveillance and target tracking etc [1]. The communication in wireless sensor networks is done using wireless transceivers, which can monitor noise levels, vehicular movements, lighting conditions, humidity, pressure and temperature [3].

In general, traditional networks support point-to-point or point-to multipoint data communication. WSNs have the ability to work virtually in any physical environment, where wired connections are impossible. They are deployed to sense, process and disseminate information of any targeted environments. Before network deployment the location of nodes is not specified and this capability allows us to spread them in remote and dangerous areas. In order to protect the nodes, the self-organizing protocols and algorithms are used. Basically, the battery-operated sensor devices of WSNs are equipped with data processing, computing and data communicating components. Conventional wireless sensor networks are prone to additional threats which results from intrinsic characteristics of sensor nodes such as CPU cycles, battery capacity, memory, deployment environment and, communication bandwidth. Because of these intrinsic properties of sensor nodes traditional security mechanisms for providing authentication, availability and confidentiality are inefficient for wireless sensor networks.

The major challenges for employing efficient security mechanism in WSNs are created by the size, memory, processing power of the sensors. The lack of power and data storage initiates severe resource constraints in WSNs. Both are major obstacles towards the traditional security implementation techniques [4].

Considering this many researchers started dealing with the challenges of energy funds and maximize the processing power of sensor nodes. Surveillance and monitoring are the prime factors in controlled environment. Whereas sensor network security becomes extremely important in uncontrolled environment. Even though wireless sensor networks assure large number of applications there are many problems of securing these networks. The major preferences in wireless sensor networks are modelling and routing strategies, yet security issues are of extensive focus. Sensor networks are

predominantly prone to several kinds of attacks [1].

They are executed in a variety of ways, most remarkably as DoS attacks, physical attacks, violation of privacy, traffic analysis and so on. Majority of the attacks in opposition to WSNs are due the inclusion of false information by the compromised nodes of the network. A mobile agent-based security system is developed for defending and detecting the false reports by compromised nodes [5]. In recent times, mobile agent based computing prototype has become an activist in the perspective of wireless sensor networks. A mobile agent is defined as an autonomous software component which acts like a thread or a programming segment. This is self-controlling and migrates among the nodes following an itinerary and carries out the data computation [6].

This paper outlines the security issues and challenges of wireless sensor networks and confers the critical parameters. Very first we introduce the obstacles and security requirements of WSNs. Later summarizes the security treats and sufficient defensive mechanisms. Finally, the importance of introducing mobile agent-based software prototype is pointed out.

1.1 Significance of the Paper

The benefits of this paper to the people of Ghana as well as other researchers in the same field are as follows:

1. The paper will unveil the benefits of WSN on information security to clients in LAN environment.
2. The findings of the study will help ICT personnel and their clients to know the security challenges of WSN and how to solve them.
3. The paper will unravel the information security challenges faced in WSN computing in Ghana.
4. The findings of the paper will help people to know how to solve or reduce information security risks in WSN computing in Ghana.
5. The findings of the paper will guide the managers of IT companies and other authorities to know the information security risks their clients faced in WSN computing.
6. The findings of the paper will also serve as a guide to software institutions to protect their data from fraud in Ghana.
7. Lastly, it will be useful to future researchers who will like to conduct a similar research in the same field.

2. LITERATURE REVIEW

2.1 Sensor Security Obstacles

As compared to the traditional network, wireless sensor network has several constraints. Because of this it is hard to directly utilize the existing security mechanisms for WSNs. While developing functional security mechanisms following constraints are considered [7].

2.1.1 Limited resources

Implementation of the security approaches require amount of resources like memory and power. These resources are not adequate in wireless sensors.

- Limited memory and storage space: Sensors have less memory and storage capacity.
- Power limitation: Wireless sensor capabilities have biggest energy constraints.

Unreliable Communication: This is one of the most important threats in sensor network security and network security seriously relies on protocols. This in turn heavily depends on the communication.

- Unreliable transfer: Wireless sensor network uses connectionless environment for packet-based routing which is intrinsically unreliable. Due to the heavy congestion on the channel the packets may get damaged or even the packet loss may occur.
- Conflicts: Even though we have reliable channel, sometimes communication goes unreliable due to WSNs broadcast nature [1].
- Latency: Node processing, congestion and multi-hop routing increases the network latency. It makes sensor nodes synchronization bit difficult.

Unattended Operation: The functionality of the sensor network plays a very important role, in making the sensor node unattended for a period of time. Main warnings of unattended sensor nodes are:

- Exposure to physical attacks: Sensor nodes are deployed in adversary dominated environment.
- Managed remotely: Sensor network remote monitoring makes it impossible to identify the issues of physical tamper and maintenance.
- Lack of central management point: Absence of central management point in the distributed sensor network.

2.2 Security Requirements in Wireless Sensor Networks

The resource limitations of wireless communications are sensor nodes, size, topology and density of the network. These are of high security challenges in WSNs. Ultimate security requirements of WSNs are authenticity, integrity and confidentiality.

Cryptography: Traditionally developed encryption-decryption techniques are not feasible enough to use directly on WSNs. Some critical questions like how keys are generated, managed and revoked will arise while applying encryption and decryption techniques to WSNs. Encryption schemes in WSNs require transmission of extra bits that consumes more power from the tiny sensors. Extra processing power, memory and battery are the basic parametric resources which improves the longevity of the sensors [5]. This type of security schemes also increases jitter, delay and packet loss in WSNs [7]. For the most secured communications of the WSNs all the messages are encrypted and authenticated. Security attacks on the flow of information can be prevalent. Due to uncontrolled node of environments and nature of wireless channels, the information is vulnerable to modification. An adversary can make use of any kind of cryptographic impairments for modification of the data and make information unavailable.

Steganography: As cryptography deals with hiding the message content, steganography deals with hiding the message existence [8]. The art of steganography deals with embedding a message within a multimedia data like image, audio and video. Steganography and multimedia processing are not related to securing wireless sensor networks because of the insufficient sensor resources. Basic security requirements of WSNs are data availability, confidentiality, authentication, integrity and nonrepudiation.

Data Availability: Modifying the legacy encryption schemes to work within the WSN is complicated and expensive. Few approaches enforce severe limitations on the data access to simplify the algorithms.

These approaches reduce the sensor networks availability for the below reasons:

- Additional computation and communication consume extra energy.
- The availability of the network is greatly threatened by single point failure.

Data Confidentiality: Is the most significant issue in network security. Confidentiality in the sensor networks relates to the following:

- A sensor network should not disclose the data to any neighborhoods.
- Example like military applications requires high confidentiality in data storage.
- For sensitive data communication having a secure channel is highly important.
- Sensor information is encrypted to safe guard against the traffic analysis.
- Thus, confidentiality is achieved by encrypting the sensitive data by sharing the secrete key between sender and recipient [9].

Data Integrity: Even though, the confidentiality protects the information from the adversary, it doesn't mean that information is secured. Attackers have the ability modify the information. A malicious node may send the manipulated data to the original receiver. In harsh communication environment, the data loss may occur even in the absence of the malicious node. The received data has not been altered in transit can be assured by data integrity.

Authentication: An attacker not only has the capability to change the data packet. Even it has the ability to modify the entire data stream by adding the extra packets. Therefore, the duty of the receiver has to ensure the correct source. While constructing the sensor networks, authentication process is essential for many applications. Symmetric encryption mechanism assures the data authentication in case of two-party communication. Message authentication code is calculated by sharing the secret key between sender and receiver.

Data Freshness: Though the integrity and confidentiality are assured, we have to make sure regarding the data freshness. This implies that the data is recent and no adversary has

replayed with old messages. If the design is using a shared key strategy the freshness requirement is very important. Monotonically counter is incremented with every message and the messages with old counter values are rejected. As per literature we have two types of freshness: weak freshness carries no delay but offers partial message ordering, and strong freshness provides delay estimation and offer a total order [5].

Robustness and Survivability: The sensor networks should be strong enough to withstand the security attacks and even if the attack is successful, the effect must be very less. Vulnerability of a node should not breach the entire network security.

2.3 Security Threats in Wireless Sensor Networks

Broadcast nature of the transmission channel makes wireless networks highly susceptible to different types of security attacks. Eavesdropping is easy because of the broadcast nature of the wireless communication. As compared to the guided transmission channel communications over unguided transmission channel is more vulnerable to security attacks. Typical sensor nodes mounted in a large area are liable to security threats. It is highly impractical to scrutinize and guard each and every individual sensor node in a network against logical or physical attacks. Sensor networks predominantly vulnerable to many types of attacks like physical attacks, denial of service attacks, traffic analysis and node replication attack and so on.

Denial of Service Denials of service attacks are formed by the malicious action or accidental failure of nodes. By the transmission of the unnecessary packets, DoS attacks tries to drain the resources available at the victim nodes. Thus, legitimate network users are prevented from accessing the service. In an extent Denials of Service can diminishes a network's capacity to provide defined services. DoS attacks are performed in different layers in wireless sensor networks.

Tampering and jamming are at the physical layer, exhaustion and collision are at the data link layer, hello flood, warm hole, sink hole, sybil attack and selective forwarding are belongs to network layer, malicious flooding belongs to transport layer and clone attack is at the application layer. The defensive technique to prevent DoS attacks includes effective key management schemes, rate limitation, error correction, strong identification and authentication of traffic.

Sinkhole Attack: An adversary draws whole traffic towards compromised node. A metaphorical sinkhole is created as adversary draw traffic from specific region through a compromised node, which makes entire traffic, has to go through an adversary. This attack can even facilitate other kind of attacks like selective flooding and be able affect the nodes located at far away distance to the base station.

Cloning Attack: This acts like a starting point to span various dangerous attacks. In cloning attack environment an adversary with a compromised node credentials secretly launch the replicas of the node into the network. As these replicas are used to introduce different types of attacks the aim of the sensor applications are threatened.

Wormhole Attack: In the critical wormhole, attack adversary records the messages at one location of the network and tunnels to another location through a low latency channel. As wormhole attack may not necessitate a compromising node in the network, makes this attack a significant one in WSNs. When sensor node 1 broadcast the route request packet an adversary captures the packet and forwards to its neighborhood. Once the neighboring node receives this packet, it assumes that it is in the range of node 1 and mark it has its own parent. Thus, even though the victim node is multiloop at a distance from node 1, the attacker is able to convince that the node 1 is just a single hop apart from them, hence creates a wormhole.

Hello Flood Attack: In this HELLO packets are used like a weapon to deal with tiny sensors of the WSNs. Here adversary with high processing power and transmission range sends HELLO packets to large number of distributed sensor nodes. There by sensors are convinced that the adversary acts like their neighbor. Because of this, while transmitting the data to base station, victim node tries to go across the adversary by thinking that this may be its neighbor and eventually spoofed by the adversary

Sybil Attack: In several scenarios, the tiny sensors of wireless networks have to work collectively to complete a task; hence it demands the functionalities like subtasks distribution and

redundancy of information. In such cases, a node can act like another node by stealing the legitimate node identity. In Sybil attack a node fabricates the identities of other nodes [10]. This is very effective against the redundancy mechanisms, data aggregation, routing algorithms and resource allocation [11].

Node Replication Attack: Here by replicating the node ID of the existing sensor node, an attacker can add nodes to the existing networks. Due to such replication of the node, network's performance is severely disrupted. So, there may be a chance of packet corruption or misrouting. In turn this results in network disconnection and false readings of the sensors. Once an adversary gains physical accessibility to the whole network cryptographic keys are copied to the replicated sensors and replicated nodes are placed at the strategic points of the network [12]. Adversary has the ability to manipulate the specific segments of the network by placing the replicated nodes at the strategic points.

Layer Oriented Attacks: Wireless sensor networks are organized by layered architecture. This makes sensor networks highly vulnerable to several different types of attacks.

Physical Layer Attacks: As all higher layer functionalities rely on physical layer many attackers target this layer. Physical attacks on WSNs are like Jamming, node capturing and device tampering, etc [13]. Due to the lack of the physical control over the nodes its bit difficult to handle the physical attacks rather than software attacks.

- Jamming: This introduces powerful interference to disrupt the availability of the transmission channel.
- Eavesdropping: Without the consciousness of the sender and receiver, adversaries do the WSNs communication channels traffic analysis and gathers the data which can be used later to extract useful information [14].

Data Link Layer Attacks: The neighboring nodes coordination is the basic functionality of the link layer protocols to arbitrate the shared channel use. Adversary can violate the coordination rules and create a malicious traffic to disrupt the network operations and makes nodes vulnerable to denial of service attacks. Link layer threats are like traffic manipulation, and identity spoofing.

- Traffic manipulation: Adversary transmits the packets exactly at the same time when the authorized user does the transmission to cause the interference. Time synchronization can be done by observing the communication path and doing the calculation based on link layer protocols in effect.
- Identity spoofing: Wireless communication broadcast nature makes the identity of the sensor open to all neighboring nodes, including attackers. Due to this an attacker can forge an identity and behave like the different one.
- Device tampering: This attack leads to modify or damage the sensors physically to harm their service.

Network Layer Attacks: Network layer key concern is to position the destination and finding the optimal route to destination. Attackers can fail the communication by the packets replication and modifying the routing information. WSNs network layer is highly vulnerable to the attacks like false routing, packet replication, sinkhole attack, black hole attack, selective forwarding and wormhole attack, etc.

- False routing: False routing information is enforced to launch the false routing attacks. The different enforcement approaches are like poisoning caches, routing tables, and overflowing the routing tables [15].
- Packet replication: In the packet replication, attackers replicate the earlier received packets. Repeated broadcast of replicated packets consumes large network bandwidth and power of the node which causes the early termination of the network operations [16].

Transport Layer Attacks: An adversary repeatedly makes a new connection request until the resources reach the maximum limit. This leads to the severe resource constraints in legitimate nodes [15]. Transport layer is vulnerable to attacks like flooding and desynchronization attack [17].

- Flooding attack: These types of attacks take advantage of protocols which maintains information about the connection at both ends.
- Desynchronization attack: An adversary transmits the forged packets with spurious

information's like sequence number and control flags to interrupt an active connection.

Application Layer Attack: Application layer offers the services to the end users. As such services are time synchronization and data aggregation. Application layer is vulnerable to attacks like data aggregation distortion, clock skewing and selective message forwarding.

- Data aggregation distortion: Data processing is done at the base station, once collected data is given back to the base station by the sensor node. An adversary can change the information to be gathered and make distorted to the final computed results of the base station [18].
- Clock skewing: This attack targets the sensors, which necessitate synchronized operations [19]. An attack desynchronizes the sensors by disseminating the fake timing information.
- Selective message forwarding: This attack is initiated by forwarding the selective messages. To launch this attack in application layer, attacker must be aware regarding the semantics of the payload for selective packet forwarding [20].

2.4 Countermeasures against the Attacks

The main confront in WSNs is to provide efficient security mechanisms, by means of sensor size, processing power, memory and communication capacity [21]. Various cryptographic techniques are used for the safe communication over the sensor networks [22]. To avoid the attacks that compromise a node in getting access to the entire network, a wide variety of countermeasures and defensive mechanisms [23].

3. METHODOLOGY

The researcher adopted quantitative research design and it is a process in which numerical data is used to obtain information and consist of descriptive, correlational, experimental and quasi-experimental research. The descriptive survey was the main focus of this study and is the exploration and description of phenomena in real life situation. The study was undertaken in two IT companies in Accra in the Greater Accra Region of Ghana. The target population for the study was made up of two IT companies with one thousand one hundred (1100) workers and customers. Three hundred and forty-eight (48) customers, two managers, ten (10) administrators and secretaries for the two companies were also covered in the study.

3.1 Sampling Technique

Random sampling and purposive sampling techniques were employed to select the representative of the study. A random sampling strategy was used to select a representative number of two IT companies for the study due to the nature and the use of descriptive survey. The companies were Juma Marketing Technologies Company and Amazon Ghana Technologies. The study was limited to IT companies since participants were matured as compared to other smaller companies and as such are capable of responding to the items on the questionnaire and structured interview schedule appropriately and responsibly. In the case of the customers, eight (8) individuals were blindfolded and asked to pick a piece of paper inscription 'participant' and 'non-participant' from a basket. This method was used and applied in the companies and as such forty (40) customers were selected. As in case of workers eight (8) individuals were also blindfolded and asked to pick a piece of paper inscription 'participant' and 'non-participant' from a basket. This same procedure was used and applied in the two companies and as such forty (40) students were chosen.

The views of IT specialists were also sought. In this case all individuals were selected. Ten (10) IT specialists were selected as a result. Random sampling technique was appropriate, simple and adopted since it established homogeneity which researchers choose individuals and locations with the purpose of learning about or understanding the central phenomenon.

Purposive sampling was employed to select the administrators and secretaries of the two companies mentioned. Purposive sampling was chosen because the respondents involved were single individuals who can be hand-picked based on the purpose of the study. Purposive sampling was used to select ten (10) administrators and a secretary from the two companies. These individual respondents were selected and used to verify and cross- check responses on computer security practices in selected IT companies in Accra. The issue of triangulation in relation to the responses is ensured. The total number of samples for the study was hundred (100) respondents. This comprises forty (40) customers, forty (40) IT workers, ten (10) IT specialists, five (5) administrators and five (5)

secretaries all from the two selected IT companies.

3.2 Materials

The research instrument used for the data collection was questionnaires for the customers, workers, IT specialists, administrators and secretaries. There were thirty-two (32) items in the questionnaire for students. Questionnaire for workers was made to examine the trend of computer security practices in senior high schools. There were thirty-nine (39) items in the questionnaire for both workers and IT specialists. Questionnaire for customers was made to examine the trend of computer security practices in its companies. In addition, thirty-four (34) items were in the questionnaire for administrators and secretaries. The questionnaire examines trends of computer security practices in IT companies in Ghana. The questionnaire was arranged in 5-point Likert scale with Strongly Agree = 1, Agree= 2, Neutral = 3, Disagree = 4 and Strongly Disagree = 5.

3.3 Data Collection Procedure

The researcher visited the selected senior high schools personally with a letter to seek permission from the companies' managers as well as the cooperation of customers, workers, administrators and secretaries in order to gather the required and the necessary data for the study. Being an IT worker in the region, it was very easy to gain the support and participation of all concerned. After consultation with the respondents, agreed dates were scheduled and all were informed about the dates and the purpose of the questionnaires they were to complete. The researcher went to the selected IT companies on the said dates and administered the questionnaires. Workers, customers, administrators and secretaries were enlightened on how to respond to the items. All questionnaires were examined and clarifications made were necessary before collection.

3.4 Data Analysis

The statistical technique used for the study was descriptive statistics and this was primarily employed for the data analysis. The data obtained were computed and analysed using percentages and frequencies. The usage of a data analysis application known as the International Business Machine, Statistical Package for Social Sciences, assisted the data analysis (IBM SPSS). The respondents' responses were counted, frequencies were recorded, and a frequency distribution table was created using the data. The frequencies were transformed into percentages, which assisted in determining the various responses provided by different proportions of the study sample.

4. RESULTS AND DISCUSSION

The participants were asked to rate how much they agreed or disagreed with each of a series of statements. There were five response categories for each scale item, ranging from strongly agree to strongly disagree. The description given in text on "agree" is based on the total number and percentage that responded 'strongly agree' plus those who responded to 'agree' while those who responded to 'disagree' plus those who responded to 'strongly disagree' are together termed as "disagree" and then 'neutral' for those who have no knowledge of the question to respond. This section comprises of Tables 1, 2 and 3 and they establish the various trends of computer security practices by the customers, workers, Administrators and secretaries in the various IT companies in Accra. It brings to bear some of the security practices that are practiced in IT companies in Ghana.

Table 1 shows that 35(87.5%) of respondents agreed to the fact that they used computer with permission. The data above established that customers did not use computers anyhow in all IT companies in Accra especially IT companies that have many computers and clients. Also, it been established in Table 1 that majority 19(47.5%) of respondents attested to the fact that there is password on computers in their companies whilst only 17(43.0%) of respondents disagreed. This clearly indicated that computer security practices were strictly followed in some of the IT companies in Accra.

Data in Table 1 reveals that 27(82.5%) of respondents indicated that there are codes of conduct guiding computer usage in their schools and 5(12.5%) disagreed which indicates that a good percentage of IT companies educate their customers on what to do and what not to do when with the computers. Also, it been established in Table 1 that majority 29(72.5%) of respondents attested to the fact that network security protocols are enforced in the companies whilst only 11(26.5%) of respondents disagreed. This clearly indicated that network security protocols are enforced in some of the IT companies in Accra.

Also, it been established in Table 1 that majority 24(60%) of respondents attested to the fact that computers are used for 70% during buying and selling of goods online in the companies whilst only 16(40%) of respondents disagreed. This clearly indicated that computers are used for 70% during buying and selling of goods online in some of the IT companies in Accra. More so, it been established in Table 1 that majority 39(92.5%) of respondents attested to the fact that there are no hacking attacks occurring with the computers in the companies whilst only 1(2.5%) of respondents chose neutral. This clearly indicated that there are no hacking attacks occurring with the computers in some of the IT companies in Accra.

Table 2 indicates that majority 32(64%) of respondents emphasized that there were security passwords on computers in their companies but only 4(8%) of respondents stressed that they did not have security passwords on computers in their companies. This clearly means that schools that have computers followed security practices by putting security passwords on their computers to prevent theft and possible intrusions.

From Table 2 majority 34(68%) of respondents were neutral to the statement that vulnerability management measures were used in computers in their companies whilst very few 16(24%) of respondents also attested to the fact that vulnerability management measures were used in their schools. The result above implies that some of the IT companies in the Accra were following computer security practices whilst other schools did not. This could also be attributed to majority of workers using their personal computers in the companies and don't see why they should be vulnerable if using their personal computer.

Table 2 shows that majority 20(40%) of respondents emphasized that intrusion detective system was not used on computers in their companies to detect network attack whilst 24(48%) of respondents think otherwise were neutral. It is evidenced from the data above that computers in some of the IT companies are not protected and therefore exposed to network attacks and even to hacker's attack. Also, it been established in Table 2 that majority 35(70%) of respondents attested to the fact that network security protocols are enforced in the school whilst only 5(10%) of respondents disagreed. This clearly indicated that network security protocols are enforced in some of the IT companies in Accra.

Moreover, it been established in Table 2 that majority 39(78%) of respondents attested to the fact that computers are used for 70% during buying and selling of goods online in the school whilst only 9(18%) of respondents disagreed. This clearly indicated that computers are used for 70% during buying and selling of goods online in some of the IT companies in Accra. Also, it been established in Table 3 that all 50(100%) of respondents attested to the fact that there are no hacking attacks occurring with the computers in the companies. This clearly indicated that there are no hacking attacks occurring with the computers in some of the IT companies in Accra.

Table 1. Computer security practices by customers

Variable	SA n (%)	A n (%)	N n (%)	D n (%)	S D n (%)
Computers in my company are networked.	3(7.5)	16(40)	1(2.5)	7(17.5)	13(32.5)
There is password on computers in my company	7(17.5)	12(30)	3(7.5)	5(12.5)	13(32.5)
I use computers in my company with permission	23(57.5)	12(30)	2(5)	-	3(7.5)
I download software's and files from the internet	5(12.5)	6(15)	-	7(17.5)	22(55)
I can install any program of my computers.	4(10)	4(10)	1(2.5)	19(47.5)	12(30)
There is antivirus on computers in my company	5(12.5)	16(40)	8(20)	8(20)	3(7.5)
Antivirus on the computers is often updated	5(12.5)	10(25)	14(35)	8(20)	3(7.5)
There are security browsers on computers in my comp1	(2.5)	7(17.5)	11(27.5)	13(32.5)	8(20)
I use flash drives on computers in my company-	11(27.5)	3(7.5)	14(35)	12(30)	-
Network security protocols are enforced in my comp	13(32.5)	16(40)	1(2.5)	7(17.5)	3(7.5)
Computers are used during buying and selling	10(25)	14(35)	8(20)	3(7.5)	5(12.5)
Hacking attacks occur with the computer in my comp	1(2.5)	7(17.5)	32(80)		
There is always a teacher to help us use the computers	47.5	47.5	-	2(5)	
There are code of conduct guiding computer usage	11(40)	16(42.5)	2(5)	3(7.5)	2(5)

Table 2. Computer security practices by workers

Variable	SA n(%)	A n(%)	N n(%)	D n(%)	S D n(%)
Antivirus is used on computers in my comp	24(48)	18(36)	4(8)	4(8)	
There is security password on computers	22(44)	10(20)	14(28)	4(8)	
There is firewall on computer to prevent hackers.	4(8)	8(16)	26(52)	8(16)	4(8)
There is intrusion detective system to detect attack	6(12)	24(48)	12(24)	8(16)	
Vulnerability management measures are used	8(16)	34(68)	4(8)	4(8)	
Activation keys is installed on the computers	8(16)	10(20)	28(56)	4(8)	
Software are updated regularly	4(8)	(8)16	28(56)	10(20)	
There are special computers for workers.	8(16)	16(32)	26(52)		
Customerscan install software without login	4(8)	6(12)	14(28)	26(52)	
Workers have individual logins to the system	4(8)	8(16)	14(28)	14(28)	10(20)
Network security protocols are enforced	23(46)	12(24)	5(10)	10(20)	
Computers are used for 70% during buying and selling	22(44)	17(34)	2(4)	4(8)	5(10)
Hacking attacks occur with the computer in the company	12(24)	38(76)			
I sometimes give my login credentials to customers.	24(48)	26(52)			
I sometimes give my login credentials to workers. Workers	8(16)	16(32)	14(28)	12(24)	
allow students to enter marks into system.	4(8)	4(8)	6(12)	8(16)	28(56)

Table 3 establishes that majority 7(70%) of respondents attested to the fact that there is Antivirus is installed on computers in my school whilst only 1(10%) of respondents disagreed and 2(20%) were neutral. This clearly indicated that computer security practices were strictly followed in some of the IT companies in Accra. As indicated in Table 3 that majority 7(70%) of respondents said that they did not transfer data from one computer to another but only 4(40%) of respondents confirmed that they did transfer data from one computer to another.

Table 3 also shows that majority 6(60%) of respondents indicated that they have security passwords on their computers whilst very few 4(40%) of respondents established that they did not have security passwords on their computers. It could be observed from the data above that some of administrators and secretaries in the IT companies in Accra were strictly following the computer security practices whereas some were also not on top of computer security issues in some of the IT companies in Accra. Moreover, it been established in Table 3 that majority 8(80%) of respondents attested to the fact that network security protocols are enforced in the companies whilst only 1(10%) of respondent disagreed. This clearly indicated that network security protocols are enforced in some of the IT companies in Accra.

Also, it been established in Table 3 that all 10(100%) of respondents attested to the fact that there is no hacking attacks occurring with the computers in the companies. This clearly indicated that there is no hacking attacks occurring with the computers in some of the IT companies in Accra.

From Table 3, it is established that 7(70%) of respondents unanimously agreed to the fact that antivirus is installed on computers in their offices whilst 1(10) disagree. According to Schneier (2000), organizations such as schools and banks must inevitably come to terms with new modes of communication as well as new technological equipment and machinery that deal with topics such as result recording, completing and updating company records, and money. According to Viega & Mcgraw (2001), there is a natural push on companies to adapt to new technology such as intrusion detective instruments and tools in their computer systems. The same impulse drives teachers and account clerks who use computers in their everyday lives attach importance to the use of intrusion detective systems in their computers. Landwehr, Bull & McDermott (1993), emphasized that the defense tactics all organizations and schools are engaging to protect against the possibility of a malware today is simply inadequate. Trusted sessions, such as those between a user and a school, can be hacked or hijacked in a variety of ways. The security response to these emerging threats is shaky and ineffective. It's tentative in the sense that new threats are identified on a regular basis, and we're still far from having a complete understanding of the web application threat spectrum. Computer security is a difficult problem that requires a more complex solution than is currently available. However, one of the ways of ensuring this sophistication in data protection is by introducing artificial intelligence technology in intrusion detection systems.

Table 3. Computer security practices by administrator and secretaries

Variable	SA n (%)	A n (%)	N n (%)	D n (%)	S D n (%)
Antivirus is installed on computers in my comp	7(70)	2(20)	-	1(10)	
Software's on my computer are updated regularly	1(01)	1(10)	6(60)	2(20)	
There is security password on computers	2(20)	5(50)	-	3(30)	
There is detective system to detect network attack	5(50)	5(50)			
I transfer data from one computer to another	1(10)	5(50)	-	1(10)	3(30)
Software with activation keys.	2(20)	-	2(20)	4(40)	2(20)
I have experienced hacking on my computer	1(10)	2(20)	7(70)		
I do open strange mails and download its content.	3(30)	6(60)	1(10)		

Artificial intelligence technology facilitates and ensures effective protection of systems. Studies further corroborates this finding by stating that artificial intelligence could potentially improve radically the performance of intrusion detection systems, which directly alerts users or networks of an impending or ongoing system attacks.

What is less obvious is how to operationalize this idea in order to protect computers from attack. It is important to acknowledge that the use of artificial intelligence practice everywhere in computer security must however be strictly followed and adhered to in order to address cyber-attacks as shown in Table 3. To adequately secure the increasing amount of capability and complexity in computer security, future artificial intelligence systems involved in computer security would have to be far more advanced than anything we can fathom today.

In conclusion intrusion detective system such as artificial intelligence indeed needs to be provided in IT companies to protect confidentiality, authentication, integrity, nonrepudiation, access control, and properties of companies and institutions. According to Klein, Roff, & Hehir (2015), the most important thing to remember when it comes to computer security is to be careful of what websites you visit, what links you click on, what you enter your information into, and what you download. Antivirus software comes preinstalled on the majority of computers. For example, Windows 8 and 10 include Windows Defender, which is sufficient for the majority of users. As shown in Table 3, the study recommended Avast because it has been one of the most highly rated antivirus products for years, it does not slow down your system, and it is absolutely free. Vulnerability management, according to Cheswich & Bellon (1994), is the process of discovering, remediating, or minimizing vulnerabilities, particularly in software and hardware. Vulnerability management is crucial to network and computer security. Vulnerabilities can be found with a vulnerability scanner, which examines a computer system for known flaws such open ports, unsecured software configuration, and malware susceptibility. In addition to vulnerability scanning, many companies use professional security auditors to conduct frequent penetration testing on their systems to find flaws.

5. CONCLUSION

As WSN continue to evolve and commonly used in several high impact applications, the need for the security mechanisms become very important. WSN suffer a lot from several constraints like processing speed, memory, limited energy, unattended operations and unreliable communication etc. A variety of attacks affect the secure communication. Due to the energy depletion of the nodes network lifetime is reduced. To uphold the authenticity and data integrity measures are to be taken to resist against the attacks. Even though there are many security mechanisms the important one is the cryptographic techniques and protocols. The fundamental means of providing a security in WSNs is through the way of selecting the best suitable cryptographic technique.

A computer security practice is indispensable tool and measure to promote and improve computer use in all schools across the nation. A computer security practice is a serious issue affecting effective teaching and learning and school management in senior high schools nowadays in Ghana in general and Accra in particular and indeed need a pragmatic and urgent attention. Computer security practices should be enforced and applied in IT companies in Accra to protect companies' files, documents, personnel records, leakage of examination questions, and change of business results, duplication of files, vital properties and documents of the companies from being hacked and leaked to the public. It is therefore necessary to supply well-functioning computers that are

protected against threat in IT companies if indeed security of file document and protection of school's data and information are taken seriously.

To achieve as a result, strict computer security practices and measures must be put in place in all IT companies in Accra to prevent and protect school files, document and vital properties of the companies from hackers. In this paper, a detailed survey is given on sensor security obstacles, security requirements of WSNs, threats in wireless sensor/networks, layer-oriented attacks, countermeasures against the attacks and cited some important research issues. Anticipation to the study of this paper, the readers can have an enhanced view of various kinds of attacks, countermeasures and, defensive techniques of WSNs.

6. RECOMMENDATIONS

The study recommends that adequate and functional computers should be provided in IT companies in Accra to promote effective buying and selling online.

Also, IT specialists and mangers should be abreast with maintenance of the computers.

Furthermore, strict measures should be put in place to protect company files and documents from hackers and theft. There should be code of ethics to regulate computer use and intrusion detective devices on computers to prevent unlawful logging into company management system.

Moreover, further studies should be done on this study in different geographical area to confirm or contrast with the findings of the study. Also, future studies can look into the trend in computer usage at other IT companies in Accra.

CONSENT

The purpose of the study was not to intrude on people's privacy. Permission was requested from appropriate supporting heads and respondents associated with the study to deal with ethical issues linked with it. The study's goal was briefly described to them, and they were given the opportunity to select whether or not they wanted to participate. The information gathered was likewise kept in tight confidence, with anonymity and privacy guaranteed.

ETHICAL APPROVAL

As per international standard or university standard written ethical approval has been collected and preserved by the authors.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Communications Magazine. 2002;40: 102–114.
2. Bojkovic ZS, Bakmaz BM. In addition, Bakmaz, M. R. Security Issues in Wireless Sensor Networks. International Journal of Communications. 2008;2.
3. Carman DW, Krus PS, Matt BJ. Constraints andapproaches for distributed sensor network security. Technical Report00-010, NAI Labs, Network Associates, Inc., Glenwood, MD; 2000.
4. Chen M, Gonzalez S, Leung VC. Applications and designissues for mobile agents in wireless sensor networks. IEEE Wireless Communication. 2007;14:20–6.
5. Douceur J. The sybil attack. International Workshop on Peer-to-Peer Systems (IPTPS'02); 2002.
   Franklin M, Galil Z, Yung M. Eavesdropping games: A graph-theoretic approach to privacy in distributed systems, J.ACM. 2000;47:225–243.
6. Culler DE, Hong W. Wireless Sensor Networks. Communication of the ACM. 2004;47:30-33.
7. Karlof C, Wagner D. Secure routing in Wireless Sensor Networks: Attacks and Countermeasures, Adhoc Networks. 2003; 293-395.
8. Kurak C, McHugh J. A Cautionary Note on Image Downgrading in Computer Security Applications. Proceedings of the eighth Computer Security Applications Conference. 1992;153-159.
9. Murthy CR. In addition, Manoj BS. Transport layer and security protocols for ad hoc wireless networks. Ad Hoc Wireless Networks - Architectures and Protocols; 2004.
10. Newsome J, Shi E, Song D, Perrig A. The sybil attack in sensor networks: Analysis & defenses. Proc. Of The third international

symposium on Information Processing in Sensor Networks. 2004;259–268.
11. Parno B, Perrig A, Gligor V. Distributed detection of node replication attacks in sensor networks. In Proceedings of IEEE Symposium on Security and Privacy; 2005.
12. Pathan ASK, Islam HK, Sayeed SA, Ahmed F, Hong CS. A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks. IEEE ICNEWS; 2006.
13. Perrig A, Szewczyk R, Tygar JD, Wen V, Culler D. E. Spins: Security protocols for sensor networks. Wireless Networking. 2002;8:521–534.
14. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS Security Protocols for Sensor Networks, Wireless Networks, Eight. 2002;521-534.
15. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS: Security Protocols for Sensor Networks. International Conference on Mobile Computing and Networking (Mobi Com); 2001.
16. Xu W, et al. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. Mobile Ad Hoc Net. In addition, Comp. 2005;46–57.
17. Shi E. In addition, Perrig A. Designing secure sensor networks, IEEE Wireless Communications. 2004;11:38–43.
18. Priyanka JSA, Tephillah S, Balamurugan AM. Attacks and countermeasures in WSN. International Journal of Electronics & Communication. 2014;2.
19. Rupinder Singh Brar, Harneet Arora. Mobile agent security issues in wireless sensor networks. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). 2013;3:378-381.
20. Raymond DR. In addition, Midkiff SF. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses, IEEE Pervasive Computing. 2008;7:74-81.
21. Saleh M, Khatib IA. Throughput analysis of WE security in Ad hoc sensor networks, Proc. The Second International Conference on Innovations in Information Technology (IIT'05); 2005.
22. Santhi G, Sowmiya R. A survey on various attacks and countermeasures in wireless sensor networks. International Journal of Computer Applications. 2017;159:0975–8887.
23. Yu Y, Li K, Zhou W, Li P. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. Journal of Network and Computer Applications, Elsevier; 2011.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle4.com/review-history/74754