IOIT SECURITY ANALYSIS BASED ON GRAPH ALGORITHM

Axmadjonova M.A[1]., Jumaboyev T.A.,Nizamov A.N[2]

[1]2nd year student of the Faculty of Telecommunication Technologies and Vocational Education of the Samarkand branch of TUIT named after Muhammad al-Khwarizmi

[2]Teachers of TUIT Samarkand branch named after Muhammad al-Khwarizmi

In today's world where technology is developing at incredible speed, Internet of Things (IoT) systems are becoming an integral part of our daily lives, covering more and more aspects – from household appliances to industrial systems. This makes the importance of IoT security even more evident due to the rapidly growing number of internet-connected devices and at the same time potential threats to users and companies.

In recent times, the growing and widespread application of IoT systems has led to the emergence of specialized structures associated with these systems. Industrial IoT (IIoT) is a part of IoT in terms of applications and uses. The confluence of IoT and IIoT systems presents some integration and interoperability issues.

First, a graph-based threat detection approach is proposed for IoT-based network systems. Threat path detection is one of the most important steps in the security of IoT-based systems. A directed acyclic graph (DAG) structure is constructed using threat weights to represent weaknesses. Common threats are identified using Common Vulnerabilities and Exposures (CVEs).

Communications are secured by mutual authentication and encryption. Time-tested certificate authorities and trusted models that protect more than one billion IoT devices are used. New elliptic curve cryptography (ECC) algorithms are used to provide a high degree of security for IoT devices with limited computing resources

This study represents threats to common IoT networks through a graph structure. By using the graph structure, every threat on the network can be represented as a node.

Second, threat detection and mitigation algorithms provide better results in terms of uptime and algorithm complexity compared to George and Thampi (2018). In addition, our study was compared with Arat and Akleylek (2023a) on the threat pathway reduction procedure.

The main contributions of the study can be summarized as follows.

- This study presents a novel graph-based approach to represent common types of threats in IoT-based networks.
- Successful system security starts with risk modeling. It is unlikely to reliably protect any IT system without understanding how intruders can hack the system.
- The graph-based approach to the analysis of security threats given by George and Thampi (2018) has been modified to take into account the way threats are

identified. This modification incorporates the DFS algorithm, which is a graph-crossing or search algorithm, and finds threat paths.

• In addition, path-shortening algorithms are integrated into a compact algorithm. Modified algorithms narrow down threat paths by taking boundary values into account and compute different values in the threat path, such as cumulative threat, jump length, and hotspot values. Finally, the time complexity of identifying hot spots in the threat graph is reduced by the proposed hot spot detection method.

• The proposed approach was compared with another graph-based threat assessment model given by Arat and Akleylek (2023a) on threat pathway reduction methods. According to the results of the experiment, the proposed idea offers better uptime on procedures for finding threat pathways and detecting hot spots.

• When vulnerabilities and threats are identified, the risk of their implementation can be mitigated through efficient, reliable, and secure dynamic system governance.

Table 1.

Abbreviations and variables used throughout the article.

Variable	Description
Tahdidga Focused Graph (TDG)	IoT-based Focused Threat Graph
Src	Source node
Dest	Manzil tuguni
Graph	Generated threat graph
Visited	The node visited in the process of finding the way
Path	Each path for source and address pairs
pathList	1. List of all paths in algorithm 1
Hop	Jump Count
listOfPath	Dimensional list of all paths in algorithm 2
threatThreshold	Tahdid chegasi
remainingPath	List of ways to save the remaining roads after the roads are cut
removedPath	List of paths to maintain after roads cut
threatSum	Cumulative tahdid og'irligi
listOfPathThreat	3. Dimensional list of all threats in algorithm 3
hopThreshold	Jump length limit
adjDict	Hash object for storing node and threat pairs
hotSpotDict	Hash object to store nodes, threats, and hot spots

When a graph structure is created, the DFS algorithm is used to traverse the graph and find paths from the source to the location. The DFS algorithm works by taking an in-depth look at the neighbors of the nodes visited. If the visited node does not have child nodes, the graf crossing is completed. The DFS algorithm works using a stack structure, so it has less time and place complexity compared to the first search by latitude (BFS) algorithm.

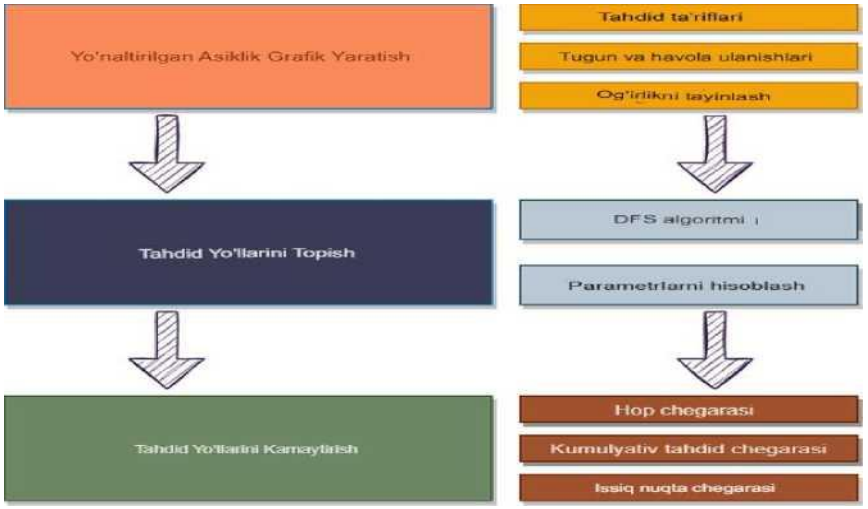

Figure 1. Main stages of the proposed idea.

These attacks and threats have been identified and classified in various databases. CVE is a database that identifies and classifies cybersecurity vulnerabilities (CVE, 2023). Various vulnerabilities and threats are identified by organizations, and CVE publishes those vulnerabilities. In this study we identify some weaknesses that are linked to our hypotheses. For example, CVE-2014-2360 is a vulnerability that could allow malicious users to execute arbitrary code. This vulnerability is present in the wireless sensor I/O modules. CVE-2022-25359 is another vulnerability found in SCADA controllers. It allows unauthenticated users to modify system file files. CVE-2022-0162 is present in some wireless router types, and an attacker could hijack router data and perform control operations through a wireless router interface. CVE-2011-2688 is a SQL server vulnerability found in web servers. CVE-2019-2776 is intended to enable an attacker to carry out Oracle database access attacks. The CVE-2021-4045 vulnerability is present in IP cameras, allowing attackers to control all camera activities. The CVE-2021-30353 vulnerability could lead to a mischeck in the Snapdragon IIoT.

LIST OF REFERENCES

1. Resolution of the Cabinet of Ministers No. 48 of 18.01.2019: On approval of the Concept of implementation of "Smart City" technologies in the Republic of Uzbekistan

2. President of the Republic of Uzbekistan Sh. Decree of M. Mirziyoyev No. PD-6079 "On approval of the Strategy "Digital Uzbekistan 2030" and measures for its effective implementation

3. Rajiv Irungbam, The Model of Smart Cities in Theory and in Practice. Journal for Studies in Management and Planning, April 2016.

URL:https://www.academia.edu/24772484/The_Model_of_Smart_Cities_in_Theory_and_in_Practice

4. Dirks, S and Keeling, M. A Vision of Smarter Cities. IBM Institute for Business Value.

2009. URL: 03.ibm.com/press/attachments/IBV_Smarter_Cities_Final.pdf