DOI:10.3233/JIFS-233759
IOS Press

An empirical analysis of evolutionary computing approaches for IoT security assessment

Vinay Kumar Sahu[a], Dhirendra Pandey[a], Priyanka Singh[b,*], Md Shamsul Haque Ansari[e], Asif Khan[c], Naushad Varish[d] and Mohd Waris Khan[c]

[a]*Department of Information Technology, Babasaheb Bhim Rao Ambedkar University, Lucknow, Uttar Pradesh, India*
[b]*CSE Department, SRM University, AP, India*
[c]*Department of Computer Application, Integral University, Lucknow, Uttar Pradesh, India*
[d]*Department of Computer Science and Engineering, GITAM (Deemed to be University), Hyderabad, Telangana, India*
[e]*Department of Computer Science Jamia Millia Islamia, New Delhi, India*

Abstract. The Internet of Things (IoT) strategy enables physical objects to easily produce, receive, and exchange data. IoT devices are getting more common in our daily lives, with diverse applications ranging from consumer sector to industrial and commercial systems. The rapid expansion and widespread use of IoT devices highlight the critical significance of solid and effective cybersecurity standards across the device development life cycle. Therefore, if vulnerability is exploited directly affects the IoT device and the applications. In this paper we investigated and assessed the various real-world critical IoT attacks/vulnerabilities that have affected IoT deployed in the commercial, industrial and consumer sectors since 2010. Subsequently, we evoke the vulnerabilities or type of attack, exploitation techniques, compromised security factors, intensity of vulnerability and impacts of the expounded real-world attacks/vulnerabilities. We first categorise how each attack affects information security parameters, and then we provide a taxonomy based on the security factors that are affected. Next, we perform a risk assessment of the security parameters that are encountered, using two well-known multi-criteria decision-making (MCDM) techniques namely Fuzzy-Analytic Hierarchy Process (F-AHP) and Fuzzy-Analytic Network Process (F-ANP) to determine the severity of severely impacted information security measures.

Keywords: IoT attacks, fuzzy-ANP, fuzzy-AHP, MCDM, IoT vulnerabilities

1. Introduction

Millions of individuals now rely on the Internet for a variety of purposes. Because of the advantages associated with the Internet, a new industry called the IoT is emerging, which allows items and devices to communicate and interact with one another through the availability of the Internet. The idea behind such technological innovation is to automate work and interconnect the devices we being used in our daily lives via the Internet. The rate at which electronic objects around us are hooked up to The internet is rapidly increasing. As per the latest Gartner report approximately 8.4 billion smart devices or things on the planet by 2020 will be deployed. This figure is

[*]Corresponding author. Priyanka Singh, Department of Computer Science and Engineering, SRM University, AP, India. E-mail: priyanka.s@srmap.edu.in.

expected to increase to 20.4 billion by the end of 2022. Machine-to-machine (M2M) interactions are projected to increase from 5.6 billion in 2016 to 27 billion in 2024.

Furthermore, many of these digital solutions enable users to consciously disclose some personal data in exchange for more innovative and personalised services. It follows that privacy and security should be prioritised in the configuration of IoT services and technologies. Sadly, this isn't the scenario for many industrial IoT products, which have insufficient, inadequate, or poorly designed security policy.

We identify a few of the most well-known and dangerous real-world IoT-related attacks, vulnerabilities, impacts, and exploitation practises carried out by various hackers in recent years. The depiction of evaluated real-world attacks is explained in section 3. Despite conducting such a thorough investigation, there are still numerous imprecise, uncertain, or partially missing pieces of information, making it difficult to determine which factor or attack is the most threatening .

In order to more effectively resolve the ambiguity that often arises in pertinent information and best reflect the inherent fuzziness of human judgment and recommendation, fuzzy set theory has been used in developing ill-defined MCDM concern. MCDM is a technique that enables you to choose the best option from a list of predestined alternatives by weighing various criteria against it. In order to deal with ambiguity in a decision-making procedures and obtain the much more consistent outcome, it is suggested to apply two different MCDM methods, namely Analytic Hierarchy Process (AHP) and Analytic Network Process (ANP), with fuzzy sets.

In both academic research and commercial practise, the AHP has now been extensively used to resolve multiple-criteria decision-making issues (such as concept assessment and equipment procurement). However, a precise pair-wise correlation with a traditional AHP might not be able to fully capture the decision-judgment maker's due to ambiguity and uncertainty in their assessment. To make up for this shortcoming in the traditional AHP, fuzzy logic is added to the pair-wise correlation in the AHP. F-AHP is the name given to this [1]. In F-ANP, the language evaluation is transformed into TFNs (triangular fuzzy numbers). In order to construct a pairwise comparison for the ANP, the TFNs have been used, and by employing extent assessment (Chan et al. 2003 [2], Chan 1999 [3]), it is possible to determine the weights for every attribute at each level. Weights are simpler to calculate in F-ANP than in traditional ANP. To deem the best application to choose, such weights could be combined [4]. In this paper, we use the F-ANP method to derive priorities from various kinds of undefined ratio scale assessments, therefore expanding the ANP's capability for making decisions in the face of ambiguity. The novelty of the work is that we deeply investigated the real world IoT attacks and the digged out the seven important affected information security factors. For more refinement we have done critical risk assessment of the seven affected security factors via two well refined MCMD techniques. Our work presents the quantitative risk assessment instead of qualitative that was not done by the researchers before in this field. This quantitative approach provides the better assessment of risk in terms of weightage of the security factors which gives the clear understanding of the severity. The result of our assessment gives the quantitative insight to the researchers for future research work in this area.

The following are the key contributions of this work:

1. First, we look at the multifarious work done in terms of strengthening security towards IoT vulnerabilities.
2. We then investigated real-world IoT attacks vulnerabilities
3. Then after investigation we addresses the affected information security factors via IoT vulnerabilities in real life scenario.
4. Conferred the critical risk assessment of affected security parameters via multiple MCDM techniques.
5. Conduct an unbiased comparison of the outcomes generated by various MCDM approaches.
6. Sets the path for future study.

The rest of this article is organized as follows: Section 2 provides some information regarding Fuzzy-MCDM techniques as well as an exploration of related work. Section 3 investigates the real-world IoT attacks/vulnerabilities. Section 4 presents the critical risk assessment of affected security parameters via multiple MCDM techniques. Section 5 represents the impartial comparison of results obtained by the multiple MCDM techniques. Section 6 portrays the discussion and suggested the future direction. Finally, author concludes the work with cogent explanation in Section 7.

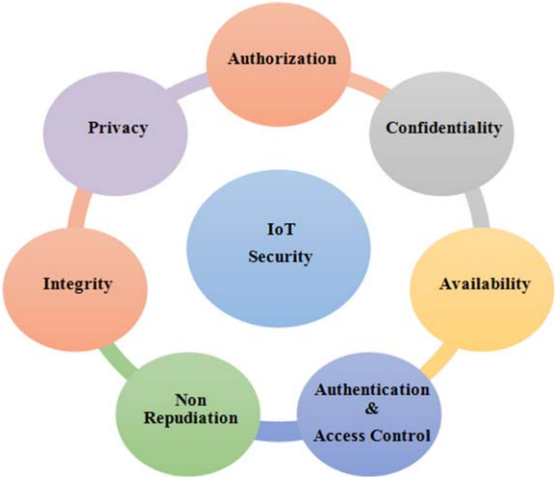

Fig. 1. Information security parameters.

2. Related works

Various IoT-empowered attacks discovered across all application domains since 2010 were surveyed by the author. The author focuses on the most recent, verifiable IoT-enabled assaults for each industry, based on reported proof-of-concept attacks and documented real-world instances [5]. The authors investigated nine real-world security events that attacked IoT devices deployed in the consumer, industrial, and commercial sectors. And presents a taxonomy that offers a systematic approach for classifying attacks based on the compromised layer and associated impact [6]. The "value-focused thinking" strategy is adopted by the researcher to systematically determine IoT security goals and values from 58 IT specialists. They provide four core goals and thirteen means goals [7]. The author provides an Organizational Information Security Framework Regarding Human Aspects contributing to the IoT, which contains remedies that can assist avoid or mitigate data breach occurrences caused by human factors [8].

The multitude of IoT devices is increasing rapidly. The legal regime for ensuring data controller as well as processor adherence must be enhanced in order to provide a safer environment for emerging creative IoT products and services without jeopardising data subjects' freedoms and rights. It is also critical to raise homeowners' awareness of potential security risks while using smart and IoT services and devices [9].

The researcher focused on a comprehensive investigation of the most common methods of attacking commercial applications, as well as the commensurate literature studies, with the goal of providing a more efficacious, cyber-security-oriented strategy that would ultimately lead to a more adaptable industrial environment. The author's major contribution is to dealing with commercial IoT technologies in general, with a major analysis on issues concerning cyber-attacks on industrial equipment, as well as the most recent mitigation strategies for the safety of the infrastructure in question, via a crucial and benchmarking schema [10].

The author demonstrates a short illustration of possible attacks on Bluetooth Low Energy (BLE) devices using several current tools to conduct spoofing, firmware assaults, and man in the middle (MITM) attacks. They also emphasised the necessity of privacy and security in BLE devices [25]. Author discusses numerous IoT security challenges such as IoT security framework, attack types, encryption challenges, authentication, and IoT hardware-based support [26].

In the research during 2004 and 2018, researchers analysed the types of threats that impact the firmware update process in IoT devices and the current secure firmware update techniques for IoT devices. A number of well-known firmware evaluation and vulnerability assessment tools are also included. They are certain that their study will enable researchers to create new defences for embedded devices by enabling firmware inspection, attacks, and security [27].

The idea of malware and botnets operating behind "Distributed" DoS in IoT is discussed by the author. The diverse DDoS defence strategies are thoroughly discussed and contrasted in order to pinpoint any security flaws. Additionally, researchers identify the unresolved problems and difficulties that must be overcome to improve DDoS prevention [28]. Researchers are working to address this discrepancy by thoroughly examining the issues and challenges related to IoT security. An in-depth review of IoT attack surfaces, security concerns, threat models, forensics, needs, and obstacles is provided by the researcher [29].

The author mentions their efforts to comprehend file less exploits on Linux-based Iot systems in the wild. They deployed four hardware IoT honeypots and 108 specifically developed software IoT honeypots over the course of a year, effectively attracting a wide range of real-world IoT threats. They discuss their measuring analysis on these attacks, focusing on file less attacks, including the prevalence, environments, exploits, and impacts. The research also yields multiple insights into effective defensive techniques that IoT providers and end users can implement [30].

The author provides a high-level overview of the security threats in the IoT sector and discusses some potential countermeasures. Then, describes and analyses some of the attacks against real IoT devices documented in the literature, highlighting the present security flaws of commercial IoT solutions and emphasising the significance of addressing security as an important component of IoT system design [31]. The author discovers that the Analytic Hierarchy Process (AHP) and approach for Order of Preference by Similarity to Ideal Solution (TOPSIS) hesitant fuzzy-based symmetry approach is an efficient methodology for analysing the endurance of online applications. The authors analysed the outputs of six distinct University projects to determine the level of accuracy of the results and their sensitivity [32].

Researchers deductively and inductively identify attack traits and measurements based on the most recent research and a collection of roughly 50 attacks. The author uses a real-world situation involving a German steel factory to illustrate the utility and practical significance of their taxonomy. [33]. K. Sahu et al. proposed a unique technique for selecting the optimal model of dependability prediction. The methodology is an amalgam of the AHP, hesitant fuzzy sets (HF), and the the technique for order of reference by similarity to ideal solution (TOPSIS) [34].

Ling Z. et al. provides an overview of IoT privacy and security as well as a case analysis. Their contribution is dual in nature. First, they show their end-to-end perspective of an IoT system. Second, they give a vulnerability assessment of the Edimax IP camera system using an end-to-end view of IoT privacy and security. Their real-world trials confirm the efficacy of the revealed attacks and increase the stakes for IoT makers once more [35]. The researcher was trying to figure out and rank different ways of handling security problems. They wanted to do this by going through two known approaches that people use when trying to analyze big data security. The author is currently using the Fuzzy AHP approach to see how much levels of priority matter in the realm of data security [36].

As per the outcomes of this study, sit may be possible to use F-ANP to obtain a distinct set of attributes that are more pertinent for assessing the importance of security attributes with respect to test plan parameters. This article reviews the information that was gathered from a range of experts who work in academia as well as industry. To assess the significance of particular security qualities, the efforts of such experts are subjected to a weighing and ranking procedure using a risk assessment plan formulation. As a result, F-ANP uses the evaluative contributions from a group of decision-makers to develop a network of security parameters including test plan criteria based on their level of significance or priority. Additionally, F-ANP has established a more precise relationship that enables the decision-makers to finish the priority evaluation.

3. Expounding real world IoT attacks

We have considered some famous and critical real world IoT attacks of last few years. The illustration of considered real world attacks are tabulated in Table 1. These are just a couple of drops in an ocean of unprotected devices and gizmos in which we are all drowning.

4. Risk assessment of encountered security parameters using MCDM techniques

The cases that are uncovered in section 3 bring to the fore the inherent security issues with IoT systems and show how such interconnected ecosystems might be vulnerable to attack. We investigate IoT-enabled cyber assaults found across all application areas. We focus on the most recent, certified IoT-enabled assaults in each industry, based on documented real-world instances and written proof-of-concept assaults. After extensive investigation, we found that several information security factors were affected, which are as follows: Confidentiality, Integrity, Availability, Privacy, Access Control, Authorization and Non-Repudiation. We accord a complete attack assessment on IoT devices, as well as their extant threat scenario.

To enhance the accuracy and acceptability of the evaluation, the risk assessment of encountered security factors was performed using two distinct MCDM techniques, namely F-AHP and F-ANP. Now the MCDM methodologies are employed and all the encountered security factors are mapped to respective variables to make the calculation easier and effective. The mapping of the security factors is illustrated as follows: Availability as S1, Access control as S2,

Table 1
Real world IoT attacks

S. No.	IoT Attacks	Year	Reported by	Type of Vulnerability(s)	Compromised Security Factors
[11]	Stuxnet	2010	Sergey Ulasen	Worm attack and Affects the supervisory control and data acquisition (SCADA) systems	Access Control and Data Theft
[12]	The TRENDnet Webcam Hack	2012	Report by TechNewsWorld	Network data transfer without encryption	privacy, confidentiality or integrity
[13]	The Jeep Hack	2015	Black Hat security researchers Charlie Miller & Chris Valasek	Access Control	Access Control
[14]	The Owlet WiFi Baby Heart Monitor Vulnerabilities	2016	security researcher Jonathan Zdziarski	Unencrypted data transfer over network	Authentication and Access Control
[15]	VPNFilter	2018	security researchers from Cisco Talos	Malware attack: that has the ability to steal data, a kill switch that can be used to instantly deactivate the compromised router, and the ability to survive router reboots.	Integrity, Access control
[16]	Nortek Security & Control – Access Control System Breach	2019	Applied Risk	Malware and DoS attack	Access Control
[17]	The Big One: The Apache Log4j Vulnerability	2021	Chen Zhaojun of Alibaba Cloud Security Team	Remote code execution (RCE)	Confidentiality, Integrity, Availability, Access Control
[18]	BotenaGo	2021	AT&T Alien Labs	Malware, RCE and Botnet attack	Confidentiality, Integrity, Availability, Access Control
[19]	GOautodial vulnerabilities	2021	Scott Tolley of theâŁ¯SynopsysâŁ¯Cybersecurity Research Center	Information disclosure and RCE	Confidentiality, Integrity, Availability, Access Control
[20]	COMELEC (The Commission on Elections) hack	2022	Manila Bulletin (MB) Technews team	Breach the servers	Access Control
[21]	Critical PTC Axeda bugs jeopardise healthcare, IoT devices	2022	Vedere Labs and CyberMDX	Information Disclosure, DoS, RCE	Integrity, Confidentiality, Availability, Access Control
[22]	Jacuzzi SmartTub web bugs (Jacuzzi Hot Tubs)	2022	Eaton Zveare	View and potentially manipulate the personal data	Access Control
[23]	Grand hack auto	2023	security researcher Sam Curry	account takeover, remote code execution (RCE), and even hijacking physical commands	Integrity, Confidentiality, Access Control
[24]	BlackCat's Sphynx Ransomware	2023	Microsoft	credential dumping, remote command-execution (RCE)	Confidentiality, Integrity, Availability, Access Control

Confidentiality as S3, Integrity as S4, Privacy as S5, Authorization as S6 and Non-Repudiation as S7.

4.1. Fuzzy analytic hierarchy process

The AHP has now been extensively utilized in both scientific research and industry practise to handle multiple-criteria decision-making challenges (e.g., concept appraisal, equipment selection). A precise pair-wise comparison for a conventional AHP, however, would not be able to fully reflect the decision-maker's opinion due to uncertainty and vagueness in their assessment. As a result, to compensate for this shortcoming in the standard AHP, fuzzy logic is included into the pair-wise comparison in the AHP. This envisaged as F-AHP [37].

Since the core AHP doesn't really allow for subjective judgments, the fuzzy logic method has contributed to improving it. In F-AHP, pairwise comparisons among both alternatives and criteria are accomplished using linguistic terms encoded by triangular numbers [38]. Van Laarhoven and Pedrycz developed one of the earliest F-AHP implementations [39]. For pair - wise comparisons, they devised the triangle membership functions. Following that, Buckley [40] made a contribution to the discussion by identifying the fuzziness of comparison ratios with triangle membership functions. The use of triangular figures in pair-wise comparisons is another novel technique that Chang [41] introduced. Even though F-AHP contains different methods, in the context of this research Buckley's methods [40] are used to calculate the relative relevance weights for the alternatives and the criteria.

The following are the process steps:

Step 1: The criteria and alternatives are compared by the Decision Maker using the linguistic terminology indicated in Table 2.

Table 2
Linguistic terms and the corresponding TFN

Saaty scale	Definition	Fuzzy Triangular scale
1	Equally important (Eq. Imp.)	(1, 1, 1)
3	Weakly important (W. Imp.)	(2, 3, 4)
5	Fairly important (F. Imp.)	(4, 5, 6)
7	Strongly important (S. Imp.)	(6, 7, 8)
9	Absolutely important (A. Imp.)	(9, 9, 9)
2	The intermittent values between two adjacent scales	(1, 2, 3)
4		(3, 4, 5)
6		(5, 6, 7)
8		(7, 8, 9)

Table 3
Pair wise comparison matrix of affected security factors (AHP)

Security Factors	**S1**	**S2**	S3	S4	S5	S6	S7
S1	1	1.064, 1.529, 1.990	0.511, 0.598, 0.859	1.729, 2.311, 2.901	1.692, 2.414, 3.147	1.576, 2.093, 2.613	0.552, 0.639, 0.905
S2	–	1	1.182, 1.474, 1.872	0.791, 0.960, 1.135	1.459, 1.859, 2.215	1.333, 1.523, 1.797	1.553, 2.200, 2.850
S3	–	–	1	1.085, 1.343, 1.872	1.605, 2.336, 3.147	0.335, 0.427, 0.574	1.399, 1.816, 2.446
S4	–	–	–	1	1.496, 1.928, 2.354	0.945, 1.081, 1.637	1.250, 1.639, 2.028
S5	–	–	–	–	1	1.187, 1.535, 2.028	1.192, 1.489, 1.898
S6	–	–	–	–	–	1	0.398, 0.511, 0.662
S7	–	–	–	–	–	–	1

Table 4
Defuzzyfication of local priorities (using alpha cut method)

Security Factors	S1	S2	S3	S4	S5	S6	S7	Weightage
S1	1	1.778	0.892	2.563	2.667	2.344	0.934	0.218993
S2	0.562	1	1.751	1.212	1.853	1.794	2.415	0.17967
S3	1.121	0.571	1	0.989	2.606	0.691	2.120	0.155693
S4	0.390	0.825	1.011	1	2.177	0.771	1.890	0.133659
S5	0.375	0.540	0.384	0.459	1	1.821	1.767	0.102951
S6	0.427	0.557	1.447	1.297	0.549	1	1.436	0.118589
S7	1.071	0.414	0.472	0.529	0.566	0.696	1	0.0904455
								CI= 0.0943425

As per the corresponding TFNs of these linguistic notions, for instance, the fuzzy triangular scale is used if the decision maker says that “Criterion 1 (C1) is Weakly Important than Criterion 2 (C2)” (2, 3, 4). In contrast, the assessment of C2 to C1 will use the fuzzy triangular scale of (1/4, 1/3, 1/2) in the pair wise contribution matrices pertaining to the criteria.

The pair wise contribution matrice is illustrated in Equation 1, where $\widetilde{\mathrm{P}}^q_{mn}$ represents the q^{th} decision makers’ preference of m^{th} criterion over n^{th} criterion, via TFN. In this scenario, “tilde” stands for the triangular number demonstration, and “p” stands for the primary decision maker’s precedence of the first over the second criterion, and equals to $\widetilde{\mathrm{P}}^1_{12} = (2, 3, 4)$.

$$\widetilde{X} = \begin{bmatrix} \widetilde{\mathrm{P}}^q_{11} & \widetilde{\mathrm{P}}^q_{12} & \ldots & \widetilde{\mathrm{P}}^q_{1j} \\ \widetilde{\mathrm{P}}^q_{21} & \ldots & \ldots & \widetilde{\mathrm{P}}^q_{2j} \\ \ldots & \ldots & \ldots & \ldots \\ \widetilde{\mathrm{P}}^q_{j1} & \widetilde{\mathrm{P}}^q_{j2} & \ldots & \widetilde{\mathrm{P}}^q_{jj} \end{bmatrix} \ldots\ldots\ldots..(1)$$

Step 2: If there are many decision-makers, the preferences of each one are averaged $(\widetilde{\mathrm{P}}^q_{mn})$, and the $(\widetilde{\mathrm{P}}_{mn})$ is determined according to Equation 2.

$$\widetilde{\mathrm{P}}_{mn} = \frac{\sum_{q=1}^{q} \widetilde{\mathrm{P}}^q_{mn}}{q} \ldots\ldots\ldots(2)$$

Step 3: Pair-wise contribution matrices are updated in accordance with averaged preferences, as indicated in Equation 3.

$$\widetilde{X} = \begin{bmatrix} \widetilde{\mathrm{P}}_{11} & \ldots & \widetilde{\mathrm{P}}_{1j} \\ \vdots & \ddots & \vdots \\ \widetilde{\mathrm{P}}_{j1} & \ldots & \widetilde{\mathrm{P}}_{jj} \end{bmatrix} \ldots..(3)$$

Step 4: As per Buckley [40], the geometric mean of each criterion’s fuzzy comparison values is determined as given in Equation 4. Here, $\widetilde{\mathrm{k}}_m$ still indicates triangular values.

$$\widetilde{\mathrm{k}}_m = \left(\prod_{n=1}^{j} \widetilde{\mathrm{P}}_{mn}\right)^{1/j}, m = 1, 2, ..., j \qquad \ldots(4)$$

Step 5: To calculate the fuzzy weights of each criterion, Equation 5 is used by incorporating the following three sub-steps.

Step 5a: Determine the vector sum of each $\widetilde{\mathrm{k}}_m$.

Step 5b: Find the (–1) power of the summation vector. To make it in order of increasing, replace the TFN.

Step 5c: To determine the fuzzy weight of the criterion $m(\widetilde{\mathrm{g}}_m)$, multiply each $\widetilde{\mathrm{k}}_m$ with this reverse vector

$$g_m = \widetilde{k}_m \otimes (\widetilde{k}_1 \otimes \widetilde{k}_2 \otimes \ldots \otimes \widetilde{k}_j)^{-1}$$

$$= (hg_m, ig_m, lg_m) \qquad \ldots(5)$$

Step 6: As $\widetilde{\mathrm{g}}_m$ are still TFN, they must be defuzzified using the Centre of area approach given by Chou and Chang [42], using Equation 6.

$$W_m = \frac{hg_m, ig_m, lg_m}{3} \qquad \ldots(6)$$

Step 7: W_m is a non-fuzzy number. However, it must be normalized using Equation 7.

$$V_m = \frac{W_m}{\sum_{m=1}^{j} W_m} \qquad \ldots(7)$$

These seven steps are followed to determine the normalised weights of both criteria and alternatives. The scores for each alternative are then determined by multiplying each alternative weight by the corresponding criteria. According to these findings, the option with the highest score is recommended to the decision makers. In this investigation, the findings are compiled by first obtaining the viewpoints of a variety of recognized authorities in the subject and then computing an average of those individuals’ points of

Table 5
Supermatrix formed by local priorities vectors

Security Factors	S1	S2	S3	S4	S5	S6	S7
S1	1	0.2688	0.1300	0.2716	0.2400	0.3040	0.2228
S2	0.2920	1	0.3059	0.2551	0.2889	0.2349	0.2319
S3	0.2567	0.2505	1	0.2192	0.1550	0.2200	0.2200
S4	0.2299	0.2277	0.2319	1	0.1308	0.0602	0.1182
S5	0.1527	0.1593	0.0886	0.1656	1	0.0705	0.0265
S6	0.0687	0.0937	0.0232	0.0887	0.0754	1	0. 1805
S7	0	0	0.2203	0	0.1400	0.1105	1

Table 6
Weighted supermatrix

Security Factors	S1	S2	S3	S4	S5	S6	S7
S1	0.5	0.1344	0.065	0.1358	0.1182	0.152	0.1114
S2	0.146	0.5	0.153	0.1275	0.1423	0.1174	0.116
S3	0.1238	0.1253	0.5	0.106	0.0764	0.11	0.11
S4	0.115	0.1139	0.116	0.5	0.0644	0.0301	0.0591
S5	0.0764	0.0796	0.0443	0.0828	0.04926	0.0352	0.0133
S6	0.0343	0.0496	0.0116	0.0443	0.0371	0.5	0.0903
S7	0	0	0.1102	0	0.069	0.0552	0.5

Table 7
Limit supermatrix

Security Factors	S1	S2	S3	S4	S5	S6	S7
S1	0.1888	0.1888	0.1888	0.1888	0.1888	0.1888	0.1888
S2	0.2166	0.2166	0.2166	0.2166	0.2166	0.2166	0.2166
S3	0.1852	0.1852	0.1852	0.1852	0.1852	0.1852	0.1852
S4	0.1619	0.1619	0.1619	0.1619	0.1619	0.1619	0.1619
S5	0.1117	0.1117	0.1117	0.1117	0.1117	0.1116	0.1116
S6	0.0718	0.0718	0.0718	0.0718	0.0718	0.0718	0.0718
S7	0.0641	0.0641	0.0642	0.0641	0.0641	0.0642	0.0641

Table 8
Affected security factors using F-AHP

Security factors	Global priorities
Availability (S1)	18.88%
Access control (S2)	21.66%
Confidentiality (S3)	18.52%
Integrity (S4)	16.19%
Privacy (S5)	11.17%
Authorization (S6)	7.18%
Non-Repudiation (S7)	6.41%

view. These data have been produced with the assistance of professionals working in the relevant field as well as academicians, and as a result, we are able to obtain the priority of security factors.

4.2. *Fuzzy Analytic Network Process (F-ANP)*

The ANP provides the most exhaustive framework for analysing social, corporate and governmental decisions available to decision-makers today. It is an approach that enables one to consider all of the tangible and intangible variables and factors that have an impact on making the optimal option. The ANP permits feedback and interaction both within and across clusters of elements (both inner dependence and outer dependence). Such feedback best depicts the complex consequences of human society's interplay, primarily when both risk and uncertainty are present [43].

The first component of an ANP model is a control sequence or network of key targets and criterion that control the communications in the system under investigation; the second component is a number of sub-networks of interactions among the problem's elements and clusters, one for every control criterion. The Global priorities of affected security factors is given below in Table 9 and the data used in the matrix has been collected from the experts of industries as well as academicians.

4.2.1. *Supermatrix*

The initial step in ANP is to evaluate the criteria throughout the entire system in order to construct

Table 9
Global priorities of affected security factors

Security Factors	S1	S2	S3	S4	S5	S6	S7	Weightage
S1	1	1.529	0.598	2.311	2.414	2.093	0.639	0.183922
S2	0.654022	1	1.474	0.96	1.859	1.523	2.2	0.168352
S3	1.67224	0.678426	1	1.343	2.336	0.427	1.816	0.164648
S4	0.432713	1.04167	0.744602	1	1.928	1.081	1.639	0.134153
S5	0.41425	0.537924	0.428082	0.518672	1	1.535	1.489	0.100619
S6	0.477783	0.656599	2.34192	0.925069	0.651466	1	0.511	0.12351
S7	1.56495	0.454545	0.550661	0.610128	0.671592	1.95695	1	0.124795

Table 10
Supermatrix formed by local priorities vectors

Security Factors	S1	S2	S3	S4	S5	S6	S7
S1	1	0.2577	0.1257	0.1984	0.2256	0.2998	0.2099
S2	0.3020	1	0.2959	0.2451	0.2789	0.2449	0.2119
S3	0.2667	0.2005	1	0.2291	0.1661	0.2323	0.2323
S4	0.2499	0.2266	0.2229	1	0.1408	0.0701	0.1272
S5	0.1617	0.1580	0.0991	0.2056	1	0.0605	0.0555
S6	0.0877	0.0737	0.0322	0.0877	0.0674	1	0. 1913
S7	0	0	0.2304	0	0.1514	0.1117	1

Table 11
Weighted supermatrix

Security Factors	S1	S2	S3	S4	S5	S6	S7
S1	0.5000	0.1433	0.0560	0.1458	0.1192	0.1630	0.1214
S2	0.1471	0.5000	0.1641	0.1267	0.1414	0.1112	0.1122
S3	0.1548	0.1243	0.5000	0.1170	0.0759	0.2211	0.1100
S4	0.1142	0.1141	0.1210	0.5000	0.0647	0.0315	0.0557
S5	0.0587	0.0786	0.0454	0.0828	0.0493	0.0354	0.0547
S6	0.0339	0.0501	0.0115	0.0451	0.0369	0.5000	0.0912
S7	0	0	0.1212	0	0.0688	0.0549	0.5000

Table 12
Limit supermatrix

Security Factors	S1	S2	S3	S4	S5	S6	S7
S1	0.1759	0.1759	0.1759	0.1759	0.1759	0.1759	0.1759
S2	0.2272	0.2272	0.2271	0.2272	0.2271	0.2272	0.2272
S3	0.1799	0.1798	0.1799	0.1799	0.1799	0.1798	0.1799
S4	0.1726	0.1726	0.1726	0.1725	0.1726	0.1726	0.1726
S5	0.1006	0.1006	0.1006	0.1005	0.1006	0.1006	0.1006
S6	0.0786	0.0786	0.0785	0.0786	0.0786	0.0785	0.0786
S7	0.0652	0.0652	0.0652	0.0652	0.0652	0.0652	0.0652

the supermatrix. It is accomplished by pair - wise comparisons by asking, "How important is a criterion in contrast towards another criterion in terms of our preferences or desires?" The relative relevance value can be calculated using a level of 1–9, with 1 representing equal importance and 9 representing great importance. We envisage that network model is made up of Hierarchy $P_h(k = 1, 2, ...i)$. For every hierarchy, P assumes that elements $d_{h1}, d2, ..., d_{hi}$ exists, so the impact of $P_h = (k = 1, 2, ...i)$ can be represented as follows:

$$M = \begin{array}{c|cccc} & P_1 & P_2 & \dots & P_i \\ \hline P_1 & M_{11} & M_{12} & ... & M_{1i} \\ P_2 & M_{21} & M_{22} & ... & M_{2i} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ P_i & M_{i1} & M_{i2} & ... & M_{ii} \end{array}$$

Table 13
Global priorities of affected security factors using F-ANP

Security factors	Global priorities
Availability (S1)	17.59 %
Access control (S2)	22.72%
Confidentiality (S3)	17.99%
Integrity (S4)	17.26%
Privacy (S5)	10.06%
Authorization (S6)	7.86%
Non-Repudiation (S7)	6.52%

Which is the basic form of the supermatrix. represents the impact of every element of the m hierarchy on the n hierarchy, which is known as a block of a supermatrix, and has the following form:

$$M_{mn} = \begin{bmatrix} M_{m_1 n_1} & M_{m_1 n_2} & \cdots & M_{m_1 n_{jn}} \\ M_{m_2 n_1} & M_{m_2 n_2} & \cdots & M_{m_2 n_{jn}} \\ \vdots & \vdots & \ddots & \vdots \\ M_{m_{j1} n_1} & M_{m_{j2} n_2} & \cdots & M_{m_{jm} n_{jn}} \end{bmatrix}$$

4.2.2. Weighted supermatrix

A supermatrix can be used to express the priorities of components in one hierarchy based on a specific criterion, which means that each and every column of each hierarchy with in supermatrix is column stochastic. The effect of other hierarchies, however, is unaffected by this criterion. As a possible consequence, the supermatrix's columns are not stochastic. It is crucial to take into account the influence of each hierarchy on the other. The process involves treating each hierarchy like an element, doing pairwise comparisons with respect to each hierarchy, and determining the relevant priorities. Assuming that b_{mn} represents the weighted influence of the m hierarchy over the n hierarchy, let

$$\overline{M} = b_{mn} M_{mn} \qquad ......(8)$$

$\overline{M}$ is denoted as a weighted supermatrix. The sum of the elements within every column of a weighted supermatrix is 1. This characteristic of a matrix is known as column stochastic [49]. To make sure that the total probability of all states implies 1, this step is quite identical to the Markov's chain idea.

4.2.3. Limited supermatrix

We wish to get the priority along each potential path in a supermatrix, or the final impact an element has on the top aim. This type of result can be obtained by solving $\overline{M}^{\infty}$,

$$\overline{M}^{\infty} = \lim_{h\to\infty} \overline{M}^{h} \qquad ...(9)$$

The weighted supermatrix is created to limiting powers, as shown in (9) to provide the global priority vector, often known as weights.

5. Comparison of results obtained by MCDM techniques

MCDM techniques are used to evaluate and select alternatives based on multiple criteria. There are several MCDM techniques available, each with its strengths and weaknesses. Here are some general comparisons of the results obtained by some commonly used MCDM techniques. When it comes to global priorities, F-AHP and F-ANP are commonly used MCDM techniques to evaluate alternatives based on multiple criteria. Overall, the choice of MCDM technique depends on the problem, the available data, and the preferences of decision-makers. In Table 14, the results obtained by the F-ANP and F-AHP in terms of Global Priorities of security factors are compared. Further the comparison of proposed work is also done with the various existing approaches where the proposed work endorse the transcendent over the existing approaches in terms of number of targeted security factors for severity evaluation.

Table 14
Comparision of results

Security factors	Global priorities by F-AHP	Global priorities by F-ANP
Availability (S1)	18.88%	17.59%
Access control (S2)	21.66%	22.72%
Confidentiality (S3)	18.52%	17.99%
Integrity (S4)	16.19%	17.26%
Privacy (S5)	11.17%	10.06%
Authorization (S6)	7.18%	7.86%
Non-Repudiation (S7)	6.41%	6.52%

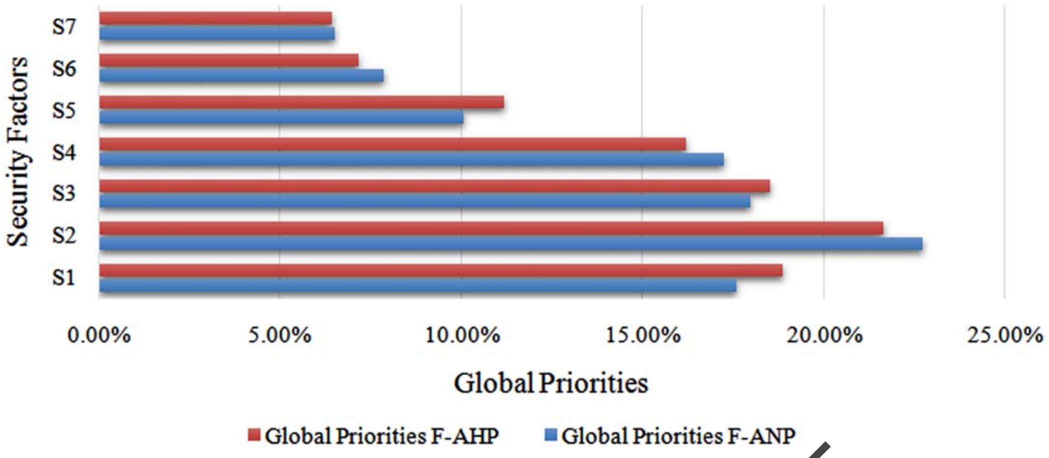

Fig. 2. Comparison of global priorities of the affected security factors.

Table 15
Comparison of proposed model with state of the art models

Breach factor	Count	Ref
confidentiality, integrity, availablility, tracebility, authenticity	06	[44]
confidentiality, integrity, availability, authentication	04	[45]
CNN + stackedauto-encoders (SAEs)	05	[1]
SVM + transient energy function (TEF)	03	[2]
Proposed Work	07	2023

6. Discussion and future research direction

The proliferation of smart, linked, and inherently insecure gadgets is altering the security landscape. Alternative strategies must be developed in addition to the clear legal structure that will be needed to accommodate the IoT technological shift.

The reason for the rising number of IoT gadgets appears to be that they offer convenience to humans and execute activities more efficiently than humans. Existing as well as forthcoming IoT solutions are highly promising in terms of increasing user comfort, efficiency, and automation. To be capable of implementing such a realm in an ever-increasing fashion, high security, privacy, authentication, and attack recovery are required. In this reference, it is critical to make the necessary modifications in the architectural style of IoT systems in order to achieve end-to-end impregnable IoT habitat.

Attacks against resource-constrained IoT systems have increased in recent years. Security breaches in IoT technologies employed in both industrial (e.g., actuators and sensors) and residential environments are constantly being revealed (e.g. implantable medical devices, home appliances, etc). Faults and malfunction in faulty hardware chips, software applications, and easily tampered devices are exacerbating the current situation.

Moreover, we have classified IoT-related security flaws, exploitation practices, attacks, and their implications via real-world cyber incidents that address IoT gadgets installed in the industrial, consumer, and commercial sectors. These (and several other) mishaps emphasize the underpinning security issues of IoT systems and illustrate the potential attack effects of such integrated ecosystems, whereas the calculated priorities of affected security factors obtained after the assessment procedure using two different MCDM methodologies, which delivers a more appropriate way to classify attacks based on the affected security factors and their corresponding impacts.

7. Conclusion

In the era of intelligent devices, IoT has expanded rapidly. A wide range of industries, including hospitals, enterprises, and farming, are heavily utilising the rapidly evolving smart gadgets, such as grids and sensors. Consumers are exposed to a wide range of security vulnerabilities because there are so many Devices connected to the internet in use. It is critical to recognize the risks that endanger the distinctive infrastructures as well as endow confidentiality of the data due to the number of threats that are escalating in the constantly evolving IoT environment and the concurrent inability of conventional security systems to recognize serious threats of intensifying depth and duration. In this paper, we demonstrate attacks/vulnerabilities of real-world IoT attack and also tabulated the impacted information security factors associated with varied vulnerabilities to concerned event in Table 1. Furthermore, the risk assessment of encountered security factors was performed by using two distinct MCDM methodologies i.e. F-AHP and F-ANP, to make assessment more accurate and appropriate. After analyzing the Global Priorities, we identify that the information security factor positioned at S2 i.e. Access Control is the most affected factor having global priority of 21.66% and 22.72% by F-AHP and F-ANP respectively among the existing factors affected in the encountered attacks/vulnerabilities and the information security factor positioned at S7 i.e. Non-Repudiation is the least affected factor having global priority of 6.41% and 6.52% by F-AHP and F-ANP respectively.

Author contributions

All authors contributed equally.

Data availability

Authors confirm that the data supporting the findings of this study are available within the article.

Declarations

Conflict of interest

The authors have no conflict of interest.

Ethical standard

This work does not require ethics approval.

Consent to participate

This work does not require consent to participate, because it does not involve human subjects.

References

[1] Z. Ayağ, A fuzzy ahp-based simulation approach to concept evaluation in a NPD environment, *IIE Transactions* **37**(9) (2005), 827–842.

[2] F. Chan, H. Chan and M. Chan, An integrated fuzzy decision support system for multicriterion decision-making problems, *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture* **217**(1) (2003), 11–27.

[3] K.-J. Zhu, Y. Jing and D.-Y. Chang, A discussion on extent analysis method and applications of fuzzy AHP, *European Journal of Operational Research* **116**(2) (1999), 450–456.

[4] R. Mohanty, R. Agarwal, A. Choudhury and M. Tiwari, A fuzzy anp-based approach to R&D project selection: a case study, *International Journal of Production Research* **43**(24) (2005), 5199–5216.

[5] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez, A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services, *IEEE Communications Surveys* & *Tutorials* **20**(4) (2018), 3453–3495.

[6] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M.K. Khan and K.-K.R. Choo, Consumer, commercial, and industrial IoT (in) security: Attack taxonomy and case studies, *IEEE Internet of Things Journal* **9**(1) (2021), 199–221.

[7] G. Dhillon, L. Carter, J. Abed and R. Sandhu, Defining objectives for securing the internet of things: A value-focused thinking approach, *WISP Proc* **3** (2016).

[8] K. Hughes-Lartey, M. Li, F.E. Botchey and Z. Qin, Human factor, a critical weak point in the information security of an organization's Internet of Things, *Heliyon* **7**(3) (2021), e06522,.

[9] G. Vojković, M. Milenković and T. Katulić, IoT and smart home data breach risks from the perspective of data protection and information security law, *Business Systems Research: International journal of the Society for Advancing Innovation and Research in Economy* **11**(3) (2020), 167–185.

[10] K. Tsiknas, D. Taketzis, K. Demertzis and C. Skianis, Cyber threats to industrial IoT: a survey on attacks and countermeasures, *IoT* **2**(1) (2021), 163–186.

[11] https://www.matisoftlabs.com/case-studies/stuxnet, accessed: 2023-07-26.

[12] https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities, accessed: 2023-07-26.

[13] https://www.kaspersky.com/blog/ blackhat-jeep-cherokee-hack-explained/9493/, accessed: 2023-07-26.

[14] https://www.theregister.com/2016/10/13/possibly_worst_iot_security_failure_yet/?mt=1476453928163, accessed: 2023-07-26.

[15] https://arstechnica.com/information-technology/2018/06/vpnfilter-malware-infecting-50000-devices-is-worse-than-/ /we-thought/, accessed: 2023-07-26.

[16] https://applied-risk.com/assets/uploads/whitepapers/Nortek-Linear-E3-Advisory-2019.pdf, accessed: 2023-07-26.

[17] https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance, accessed: 2023-07-26.

[18] https://www.bleepingcomputer.com/news/security/botenago-botnet-targets-millions-of-iot-devices-with-33//exploits/, accessed: 2023-07-26.

[19] https://portswigger.net/daily-swig/goautodial-vulnerabilities-put-call-center-network-security-on//the-line, accessed: 2023-07-26.

[20] https://portswigger.net/daily-swig/was-comelec-hacked-philippines-commission//on-elections-casts-doubt-on-data-breach-claims, accessed: 2023-07-26.

[21] https://www.forescout.com/resources/access-7-supply-chain-vulnerabilities-can-allow/

/unwelcomed-access-to-your-medical-and-iot-devices/, accessed: 2023-07-26.

[22] https://portswigger.net/daily-swig/jacuzzi-customer-details//could-be-exposed-by-smarttub-web-bugs-claims-researcher, accessed: 2023-07-26.

[23] https://portswigger.net/daily-swig/car-companies-massively-exposed-to-web-vulnerabilities, accessed: 2023-10-11.

[24] https://www.bleepingcomputer.com/news/microsoft/microsoft-blackcats-sphynx-ransomware-embeds-impacket-remcom/, accessed: 2023-10-11.

[25] S. Pallavi and V.A. Narayanan, An overview of practical attacks on BLE based IoT devices and their security, in *2019 5th international conference on advanced computing & communication systems (ICACCS)*. IEEE, 2019, pp. 694–698.

[26] A. Hameed and A. Alomary, Security issues in IoT: a survey, in *2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*. IEEE, 2019, pp. 1–5.

[27] M. Bettayeb, Q. Nasir and M.A. Talib, Firmware update attacks and security for IoT devices: Survey, in *Proceedings of the ArabWIC 6th Annual International Conference Research Track*, 2019, pp. 1–6.

[28] R. Vishwakarma and A.K. Jain, A survey of ddos attacking techniques and defence mechanisms in the IoT network, *Telecommunication Systems* **73**(1) (2020), 3–25.

[29] M.M. Hossain, M. Fotouhi and R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in *2015 IEEE world congress on services*. IEEE, 2015, pp. 21–28.

[30] F. Dang, Z. Li, Y. Liu, E. Zhai, Q. A. Chen, T. Xu, Y. Chen and J. Yang, Understanding fileless attacks on linux-based IoT devices with honeycloud, in *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, 2019, pp. 482–493.

[31] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, IoT: Internet of threats? a survey of practical security vulnerabilities in real IoT devices, *IEEE Internet of Things Journal* **6**(5) (2019), 8182–8201.

[32] K. Sahu, F.A. Alzahrani, R. Srivastava and R. Kumar, Hesitant fuzzy sets based symmetrical model of decision-making for estimating the durability of web application, *Symmetry* **12**(11) (2020), 1770.

[33] S. Berger, O. Burger and M. Roglinger, Attacks on the industrial Internet of Things-development of a multi-layer taxonomy, *Computers & Security* **93** (2020), 101790.

[34] K. Sahu, F.A. Alzahrani, R. Srivastava and R. Kumar, Evaluating the impact of prediction techniques: Software reliability perspective, *Computers, Materials & Continua* **67**(2) (2021).

[35] Z. Ling, K. Liu, Y. Xu, Y. Jin and X. Fu, An end-to-end view of IoT security and privacy, in *GLOBECOM 2017–2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–7.

[36] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B.K. Gupta and R.A. Khan, Analyzing the big data security through a unified decision-making approach, *Intelligent Automation & Soft Computing* **32**(2) (2022).

[37] M.B. Ayhan, A fuzzy AHP approach for supplier selection problem: A case study in a gear motor company, *arXiv preprint arXiv:1311.2886*, 2013.

[38] O. Kilincci and S.A. Onal, Fuzzy ahp approach for supplier selection in a washing machine company, *Expert systems with Applications* **38**(8) (2011), 9656–9664.

[39] P.J. Van Laarhoven and W. Pedrycz, A fuzzy extension of saaty's priority theory, *Fuzzy Sets and Systems* **11**(1-3) (1983), 229–241.

[40] J.J. Buckley, Fuzzy hierarchical analysis, *Fuzzy Sets and Systems* **17**(3) (1985), 233–247.

[41] D.-Y. Chang, Applications of the extent analysis method on fuzzy ahp, *European Journal of Operational Research* **95**(3) (1996), 649–655.

[42] S.-W. Chou and Y.-C. Chang, The implementation factors that influence the ERP (enterprise resource planning) benefits, *Decision Support Systems* **46**(1) (2008), 149–157.

[43] J.-Y. Wei and C.-H. Wang, A novel approach—fuzzy ANP for distribution center location, in *2009 International Conference on Machine Learning and Cybernetics*, vol. **1**. IEEE, 2009, pp. 537–542.

[44] R.O. Andrade, S.G. Yoo, I. Ortiz-Garces and J. Barriga, Security risk analysis in IoT systems through factor identification over IoT devices, *Applied Sciences* **12**(6) (2022), 2976.

[45] P. Katrakazas, T. Kallinolitou, S. Markopoulou and A. Chronopoulou, A toolchain and interoperability framework to enhance privacy and individual control at the edge, in *2022 IEEE International Smart Cities Conference (ISC2)*, IEEE, 2022, pp. 1–7.