

Does Collaborative Editing Help Mitigate Security Vulnerabilities in Crowd-Shared IoT Code Examples?

Madhu Selvaraj
University of Calgary
Canada

madhumitha.selvaraj@ucalgary.ca

Gias Uddin
University of Calgary
Canada

gias.uddin@ucalgary.ca

ABSTRACT

Background: With the proliferation of crowd-sourced developer forums, Software developers are increasingly sharing more coding solutions to programming problems with others in forums. The decentralized nature of knowledge sharing on sites has raised the concern of sharing security vulnerable code, which then can be reused into mission critical software systems - making those systems vulnerable in the process. Collaborative editing has been introduced in forums like Stack Overflow to improve the quality of the shared contents. **Aim:** In this paper, we investigate whether code editing can mitigate shared vulnerable code examples by analyzing IoT code snippets and their revisions in three Stack Exchange sites: Stack Overflow, Arduino, and Raspberry Pi. **Method:** We analyze the vulnerabilities present in shared IoT C/C++ code snippets, as C/C++ is one of the most widely used languages in mission-critical devices and low-powered IoT devices. We further analyse the revisions made to these code snippets, and their effects. **Results:** We find several vulnerabilities such as CWE 788 - Access of Memory Location After End of Buffer, in 740 code snippets. However, we find the vast majority of posts are not revised, or revisions are not made to the code snippets themselves (598 out of 740). We also find that revisions are most likely to result in no change to the number of vulnerabilities in a code snippet rather than deteriorating or improving the snippet. **Conclusions:** We conclude that the current collaborative editing system in the forums may be insufficient to help mitigate vulnerabilities in the shared code.

CCS CONCEPTS

• **Software and its engineering**; • **Security and privacy** → *Systems security*; • **Human Centered Computing** → *Collaborative and Social Computing*;

ACM Reference Format:

Madhu Selvaraj and Gias Uddin. 2022. Does Collaborative Editing Help Mitigate Security Vulnerabilities in Crowd-Shared IoT Code Examples?. In *ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM) (ESEM '22), September 19–23, 2022, Helsinki, Finland*. ACM, New York, NY, USA, 11 pages. <https://doi.org/10.1145/3544902.3546235>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ESEM '22, September 19–23, 2022, Helsinki, Finland

© 2022 Association for Computing Machinery.

ACM ISBN 978-1-4503-9427-7/22/09...\$15.00

<https://doi.org/10.1145/3544902.3546235>

1 INTRODUCTION

Crowd-sourced developer forums like Stack Overflow (SO) are popular among developers. The Stack Exchange network of sites that host Stack Overflow had 9+ billion page views from 100+ million users in 2019 alone. Stack Overflow now hosts more than 50 million posts and is visited by 11 million users per day. Questions related to coding challenges often receive code examples as solutions. Stack Overflow contains code snippets in 75% of their answers [41]. The quality of these examples and their direct reuse without modifications is a concern. Previous studies have found that 9.8% of 7,444 Stack Overflow accepted answers contained at least one instance of a poor coding practice [28], and Android code examples shared in SO are reused in millions of popular Android app [11].

Collaborative editing is introduced in forums like SO to allow users to suggest ways to improve the shared content. Previous studies offer valuable insight on the security of SO C/C++ code examples and the effect of post revisions [40–42]. However, what happens when a vulnerable code example is revised?

In this paper, we attempt to answer this question by analyzing vulnerable crowd-shared C/C++ IoT code examples. C/C++ is widely used in mission-critical systems and resource-constrained IoT devices. The Internet of Things (IoT) is an internet connected system of physical objects ("things") [17]. Rapid developments in IoT have made it so that an estimated 27.1 billion IoT devices will be connected by 2025 [30]. Increased demand for IoT in various use cases consequently increases the importance of understanding the unique challenges of IoT security [15].

The prevalence of IoT devices in our everyday life and the ease of access to such computing resources make development using IoT devices widespread. As such, recent research reports a growing number of IoT related posts in forums like SO [33, 39]. In addition, certain Stack Exchange sites are more specialized to certain fields or technologies. For example, the Arduino and Raspberry Pi sites are designed for discussion regarding development using these two tools, which are popular in the field of IoT.

We study all IoT C/C++ code snippets shared in the SO, Arduino, and Raspberry Pi Stack Exchange sites. We apply a static code vulnerability analysis tool (cppcheck) to check each code example for vulnerabilities. For each identified vulnerable code example, we collect its revision history from the three sites. We then check whether the vulnerability was introduced pre or post-revision of a code example, and whether certain revision types (e.g., code improvement) introduced or fixed vulnerabilities.

We find several severe vulnerabilities in the shared code snippets like CWE 788 - Access of Memory Location After End of Buffer. We also find that most snippets are not revised, and the majority of vulnerabilities are introduced pre code revisions. When revisions

are made, we observe that they are more likely intended to improve the functionality of the code than to make simple changes. However, these revisions often have little effect on reducing the number of vulnerabilities in a code snippet. We conclude that the current editing system in the forums may be insufficient to help mitigate vulnerabilities in the shared code snippets.

Replication Package.

<https://github.com/disa-lab/esem2022-crowdeditcodevulnerable>

2 MOTIVATING EXAMPLES

Our study was motivated by our observations of vulnerable C/C++ IoT code examples in the Stack Exchange forums. Below, we show three examples of vulnerable C/C++ IoT code snippets that were modified during revisions.

Listing 1 is an example of a SO code snippet that had vulnerabilities introduced in the original version (CWE 788 - Access of Memory Location After End of Buffer at lines 14 and 23), and then gained more vulnerabilities after it was revised, which introduced the same vulnerability (CWE 788) in line 32. Common Weakness Enumeration (CWE) is a community based list of software weaknesses maintained by the Mitre Corporation in order to help catalog software vulnerabilities [25]. As of July 2021, there are a total of 924 weaknesses in CWE Version 4.6 with 92 related to C/C++ [23, 24, 26]. In Figure 1, we show a screenshot of the official entry of CWE 788 in the CWE online database. The information contains the title of the weakness type, which is access of memory location after end of buffer. The information also contains a description with common consequences and its relationship to other CWE types. Each entry also contains examples of the vulnerability with explanations as to why it is harmful. In Figure 2, we see an example code snippet of CWE 788 as provided in the online CWE database. This vulnerability can be exploited when the C method `memcpy` is provided to copy a source memory location with a buffer. In Listing 1, the revision in line 32 to the code example calls the `memcpy` method without checking the buffer size. Therefore, instead of fixing the previous similar vulnerability in line 14, the revision has in fact made it worse.

Some code snippets did not have any weaknesses in the original version posted by the user, but then gained some as the user revised. The ARD code snippet in Listing 2 shows that an instance of CWE 788 was introduced in line 10 because the user revised to explain how to print the hexadecimal values of the array, but misused the `sprintf` function. Finally, some code snippets were also improved by revisions. For example, in a SO code snippet shown in Listing 3, the user removed an instance of CWE 788 - Access of Memory Location Before Start of Buffer in line 6 by changing the way data is stored in the data array. Therefore, revisions to code examples in online developer forums can lead to improvements, leave the code unchanged, or even make it worse by introducing further weaknesses. Our study aims to understand the proportion and types of vulnerable code examples that are mitigated through the revisions.

3 STUDY SETUP

We collect all IoT code snippets shared in three Stack Exchange sites and preprocess those to identify and record their revisions.

```
#include <iostream>
const int NR_OF_CODES = 4;
const int RADIO_ONOFF = 0;
const int CODE_LENGTH = 11;
+const unsigned char RADIO_ONOFF_ARR[] = {
+ 180,99,33,11,22,33,55, 22,22,33, 10};
int main()
{
  unsigned char codes[CODE_LENGTH][NR_OF_CODES] = { {0}, };
  std::cout << "Before:\n";
  for(int x = 0; x < CODE_LENGTH; x++){
    std::cout << static_cast<int>(codes[RADIO_ONOFF][x]) << " ",
    "\n";
  }
  codes[RADIO_ONOFF][3] = 3;
  std::cout << "\nAfter:\n";
  for(int x = 0; x < CODE_LENGTH; x++){
    std::cout << static_cast<int>(codes[RADIO_ONOFF][x]) << " ",
    "\n";
  }
  +// or try memcpy
  + memcpy(codes[RADIO_ONOFF], RADIO_ONOFF_ARR,
  + sizeof RADIO_ONOFF_ARR);

  + std::cout << "\nAfter Malloc:\n";
  + for(int x = 0; x < CODE_LENGTH; x++){
  + {
  +   std::cout << static_cast<int>(codes[
  + RADIO_ONOFF][x]) << " ", "\n";
  + }
  char c;
  std::cin >> c;
  return 0;
}
```

Listing 1: SO – 19889148 code snippet that contains a CWE 788 vulnerability in original version and deteriorated with revisions

CWE-788: Access of Memory Location After End of Buffer

Weakness ID: 788

Abstraction: Base

Structure: Simple

Status: Incomplete

Presentation Filter: Complete

Description

The software reads or writes to a buffer using an index or pointer that references a memory location after the end of the buffer.

Extended Description

This typically occurs when a pointer or its index is decremented to a position before the buffer; when pointer arithmetic results in a position before the buffer; or when a negative index is used, which generates a position before the buffer.

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	✓	119	Improper Restriction of Operations within the Bounds of a Memory Buffer
ParentOf	✓	121	Stack-based Buffer Overflow
ParentOf	✓	122	Heap-based Buffer Overflow
ParentOf	✓	126	Buffer Over-read

Relevant to the view "Software Development" (CWE-699)

Nature	Type	ID	Name
MemberOf	✓	1218	Memory Buffer Errors

Figure 1: Screenshot of CWE 788 in the CWE Database

3.1 Data Collection

We study IoT code examples shared in the following three Stack Exchange sites: SO, Arduino, Raspberry Pi. SO is the most popular Q&A site for software developers of all kinds. The other two sites are specifically setup to foster IoT-based discussions. We download the January 2022 data dump of each site, and then obtain all code examples present in answers from Arduino and Raspberry Pi. For SO, we obtain code examples from answers that belong to questions labeled as the 75 IoT-related tags from Uddin et al. [39].

Example Language: C

```
int returnChunkSize(void *) {
    /* if chunk info is valid, return the size of usable memory,
    * else, return -1 to indicate an error
    */
    ...
}
int main() {
    ...
    memcpy(destBuf, srcBuf, (returnChunkSize(destBuf)-1));
    ...
}
```

Figure 2: An example vulnerable code pattern in online CWE database that shows a CWE 788 vulnerability

```
uint8_t b[] = {0x7E, ...};
int i;
+void printHex(uint8_t num) {
+  char hexCar[2];
+
+  sprintf(hexCar, "%02X", num);
+  Serial.print(hexCar);
+}
void setup() {
    Serial.begin(9600);
}
void loop() {
    for(i=0; i<sizeof(b); i++){
-   Serial.print(b[i]);
+   printHex(b[i]);
    }
    Serial.println();
    delay(500);
}
```

Listing 2: ARD–60865 code snippet that had no vulnerabilities in original version but a revision introduced CWE 788

```
void loop() {
    char data[10];
    char indata;
    int i=0;
-   if(Serial.available() > 0) {
-       while (i<10 & data[i-1]!=13) {
-           data[i] = Serial.read();
-           i++;
-       }
-       strtouf(data,value);
-   }
+   while ((indata!=13) & (i<10)) {
+       if (Serial.available() > 0) {
+           indata = Serial.read();
+           data[i] = indata;
+           i++;
+       }
+   }
    i-=1;
    data[i] = 0; // replace carriage return with 0
    strtouf(data,value);
}
```

Listing 3: SO – 12666409 code snippet that had instance of CWE 788 but was fixed after revisions

For SO, the question tags were checked to see if they contained the keywords C or C++, and if they contained IoT related keywords.

Table 1: Statistics of each studied site

Site Name	#Code Snippets	#Post Versions
Stack Overflow (SO)	5,086	7,073
Arduino	6,906	9,393
Raspberry Pi	1,178	2,549
Total	13,170	19,015

We observed however that Arduino and Raspberry Pi questions did not have programming languages present in their tags in most cases. In order to determine the language of the code examples on these sites, we instead used the language detection tool Guesslang which has an accuracy of 90% according to its documentation [14]. Then, we used a similar approach used in previous studies to reject code snippets that only contained pseudo code by ignoring snippets that contained less than the median SO line count of 5 lines [5, 18, 42]. We also collected the entire version history of each of these code snippets. In total, we obtain 13,170 code snippets from 10,248 posts with 19,018 post versions. A breakdown of the collected snippets as well as their versions is shown in Table 1.

3.2 Data Preprocessing

The collected snippets were analyzed for weakness on the CWE (Common Weakness Enumeration) List. To do this we used cppcheck version 2.4.1 released in March 2021, which is a static code analyzer that supports various types of code checks in C and C++ code. It also allows for specific weaknesses to be suppressed. According to Zhang et al, cppcheck is able to identify 59 out of the 90 code weaknesses that are related to C and C++ [42]. Previous studies have found that cppcheck had just a 0.78 false positive rate against a test suite of 650 common C/C++ bugs [3]. Zhang et al. found that 85 out of 100 CWE instances detected by cppcheck were labelled as accurate with a strong agreement among the study’s authors (Cohen’s Kappa of 0.68) [42].

While we analyzed the initial results of running the obtained code snippets through cppcheck, we observed many instances of syntax errors. These errors are likely to be automatically detected by code editors and removed by the programmer, so we proceeded to ignore such errors in our analysis, similarly to Zhang et al., who ignored 129,395 instances of syntax errors in their initial observation of 154,198 CWE instances. Other reported errors we noticed to be unfair to deem as a weakness are CWE types such as CWE 563 - Assignment to Variable without Use. Such errors are not important as users of Q/A sites often intend to answer specific questions in code examples with direct answers, not to provide complete solutions. We therefore suppress errors in cppcheck of this nature, which are summarized in Table 2.

4 STUDY RESULTS

Our empirical study answers for research questions (RQ) to offer insights into the relationship between the vulnerability of IoT code snippets and their revisions in three Stack Exchange sites:

- (1) Were the vulnerabilities introduced through post revisions? (Section 4.1)

Table 2: Errors suppressed in cppcheck

Criteria Name	Criteria Description
Syntax Error	Errors in the syntax of the code
Unread Variable	Variable is assigned a value but never used
Unused variable or unused struct member	Variable or struct member is not assigned a value and then never used
Unused private function	Private function is not called

- (2) What are the different types of vulnerabilities found during the revisions? (Section 4.2)
- (3) Does the type of vulnerability differ depending on revision types? (Section 4.3)
- (4) Were the vulnerabilities introduced pre-edit mitigated via post revisions? (Section 4.4)

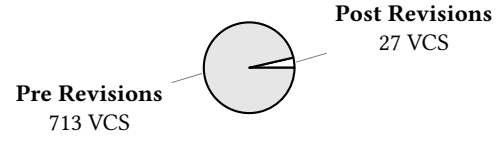
4.1 RQ₁ Were the vulnerabilities introduced through post revisions?

4.1.1 Motivation. Answers on Stack Exchange websites can be modified in order to improve its quality or to add further information. The goal of collaborative editing in the online forums is to foster content quality, which can also include improving the quality of the shared code examples. However, through these modifications, it is possible that new security vulnerabilities are introduced. An understanding of when these vulnerabilities are introduced could help us determine tools and guidelines by focusing on the timeline. For example, if most vulnerabilities are left unchanged post-edit, the collaborative editing systems needs to change.

4.1.2 Approach. To determine the stage in which a user may introduce a vulnerability in a code example, we first collect the entire version history of each post. This version history was then manually analyzed for revisions to the code examples themselves. Therefore, edits made to the text portion of the answer were not considered as revisions. We utilized this method as minor text changes such as typo fixes will have no affect on the vulnerabilities present in the code segment. After obtaining all code snippet revision history, we analyzed snippets that contained multiple versions for vulnerabilities in order to determine which version the error was introduced. Using Cppcheck to detect CWE types, we compared the results from the revised snippets with the initial ones.

4.1.3 Results. Out of our studied 13,170 code examples across the three Stack Exchange sites, we found 740 code snippets flagged as vulnerable by the cppcheck tool. We then tracked the revisions of each code snippet, and identified when the vulnerability was introduced. We find that the vast majority of vulnerabilities are introduced before edits are made to code snippets, i.e., when the code snippet was first shared. As shown in Figure 3, 713 out of the 740 vulnerable code snippets were either not changed, or contained CWE instances before revisions were made.

Table 3 shows the distribution of the vulnerable code snippets by the stage when the vulnerability was first found in the corresponding code snippet (pre or post-revisions). We see that

**Figure 3: Distribution of vulnerable code snippets (VCS) by the stage when their vulnerabilities were introduced (pre vs post revision of a code snippet)**

only a few of the vulnerable code snippets in each site were introduced post-edit, i.e., most of the snippets contained a vulnerability when the code examples were first shared. Out of the three sites, 95.8% of the vulnerable code snippets in SO had the vulnerabilities introduced pre-edit. Arduino had 96.6% of the vulnerable code snippets introduced during pre-edit and 3.4% introduced during post-edit. Finally, Raspberry Pi had no vulnerabilities introduced after revisions.

Table 3: Distribution of VCS introduced pre and post edit across the studied sites

Site	#VCS	%Pre (Black) vs. Post-edit (Red)
Stack Overflow	378	95.8% ■ 4.2%
Arduino	322	96.6% ■ 3.4%
Raspberry Pi	40	100.0% ■ 0%

Listing 4 shows a vulnerability that was not present in original version but was introduced once the user made a revision in an attempt to improve their code. In this case, an instance of CWE 398 - 7PK Code Quality in line 13 was introduced after the inclusion of a for loop that uses a variable (loop) with the same name as another function. An example of a vulnerability that was introduced before revisions and was never fixed during revisions can be found in SO post (A27918518), where an instance of CWE 401 - Missing Release of Memory after Effective Lifetime is present in line 5. Figure 4 shows the evolution of the number of CWE introduced pre and post revisions from 2009 to 2021. We find that although the number of CWEs introduced pre revisions dramatically increased between 2012 and 2016, it has been on a slight decline since. Furthermore, the number of new CWEs introduced after a revision has been made has remained relatively consistent and small.

We also find the IoT devices affected by the CWE types detected in the code snippets by analyzing the CVE descriptions of the CWE types. As shown in Fig 5, Snapdragon Consumer IoT and Snapdragon Industrial IoT are the most common affected IoT devices, followed by other devices such as GoPro cameras.

Summary of RQ1: Out of the 740 vulnerable code snippets, we find that the vast majority had vulnerabilities introduced pre code revisions (713 out of 740), which is also the case when looking at each stack exchange site individually.

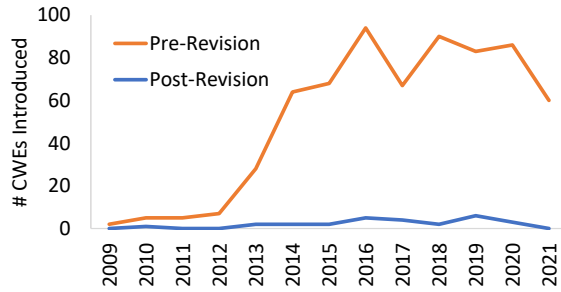


Figure 4: Evolution of #CWE instances introduced pre revisions vs. post revisions

GoProCisco_Video_Surveillance_8000_Series_IP_Cameras
Donglify
Snapdragon_Consumer_IOT
WatchGuardFirebox
Profinet
Snapdragon_Industrial_IOT
Codesys
Eclipse_IoT
Snapdragon_Industrial_IOTSIMATIC_HMI_Comfort_Outdoor_Panels

Figure 5: Common IoT Devices affected by the CWEs

```
int LED_PIN = 13;
void flashing(size_t times=1) { // By default it will flash
    once, you can chance this into your desire
    int delayPeriod = 500;
    do {
        digitalWrite(LED_PIN, HIGH);
        delay(delayPeriod);
        digitalWrite(LED_PIN, LOW);
        delay(delayPeriod);
        i++;
    } while (i<=times);
    for (size_t loop = 0; loop <
        (times*2); ++loop) {
        digitalWrite(LED_PIN, (loop % 2)?
            HIGH:LOW); // Use Modulus
        delay(delayPeriod);
    }
}
void setup() {
    pinMode(ledPin, OUTPUT);
    flashing(3);
}
void loop() {
    // Do something here
}
```

Listing 4: Revised ARD – 29060 code snippet with newly introduced instance of CWE 398 - 7PK Code Quality

4.2 RQ₂ What are the different types of vulnerabilities found during the revisions?

4.2.1 Motivation. We analyze the vulnerabilities and CWE types present in the Stack Exchange code snippets to better understand their overall security. We also aim to determine if revisions add or remove certain types of vulnerabilities in order to gain more insight on the effect of code revisions.

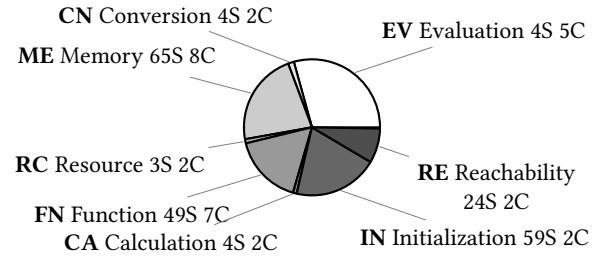


Figure 6: Distribution of the observed 30 CWE Types by the eight weakness categories (S = weak code snippet, C = CWE)

4.2.2 Approach. We use the output generated by cppcheck to determine the types of CWEs present, and the CWE database for their descriptions and characteristics. Using these characteristics, we try to understand the root cause behind the weaknesses in order to determine a categorization. This is done by both of the paper’s authors. We then check how revisions impacted the distribution of vulnerable code snippets under each category.

4.2.3 Results. Across the three stack exchange sites, we observe a total of 31 CWE types present in the 740 vulnerable code snippets (total of 1221 CWE instances), with many code snippets containing more than one CWE type. The most frequently occurring CWE type we find is CWE 398 - 7PK Code Quality, which was present in 520 code snippets. This CWE type however is not a distinct vulnerability, but instead indicates that the code snippet is of poor quality. We categorize the remaining 30 distinct CWE types based on their characteristics into the following 8 weakness categories: Evaluation - incorrect logic and comparisons, Memory - insufficient memory management, Function - improperly called and designed functions, Initialization - improperly initialized variables, Reachability - unreachable or undefined code, Resource - mismanagement of a program’s resources, Conversion - incorrect conversions of variables to different types, and Calculation - improper or incorrect calculations. In Figure 6 we observe that code snippets are more likely to contain CWE types that are evaluation, memory, and initialization related.

Among the 30 distinct CWE types shown in Table 4, we find that CWE 457 - Use of Uninitialized Variable is the most frequently occurring (detected in 49 out of 294 code snippets), followed by CWE 686 - Function Call With Incorrect Argument Type (32 out of 294).

Table 5 displays the proportion of vulnerable code snippets in each weakness category that have weaknesses introduced pre or post-edit. We find that across all categories and types, vulnerabilities are introduced more frequently before revisions are made than after, and for most categories there are no vulnerable code snippets that contain weaknesses introduced post revisions. We also observe that memory related CWE instances are more likely to be introduced by code revisions compared to evaluation related weaknesses or instances of CWE 398.

When looking at code snippets that contained vulnerabilities before revisions, but then saw a reduction in CWE instances after, we find that only 3 weakness categories (evaluation, memory, and initialization) and CWE 398 contained such snippets.

Table 4: Distribution of CWE Types by number of VCS (= Vulnerable Code Snippet). Pre = Black bar, Post = Red bar

CWE Type	Cat.	#VCS	% Pre vs. Post
398: Code Quality	–	520	████████████████████
457: Use of Uninit.Var.	IN	49	████████████████████
686: Func. Call With Incorr. Arg. Type	FN	32	████████████████████
595: Comparison of Object Refs.	EV	30	████████████████████
571: Expression is Always True	EV	30	████████████████████
788: Access of Mem. Loc. After Buff.	ME	28	████████████████████
570: Expression is Always False	EV	17	████████████████████
758: Reliance on Undefined Behavior	RC	16	████████████████████
562: Return Stack Var. Address	ME	11	████████████████████
665: Improper Initialization	IN	10	████████████████████
561: Dead Code	RC	8	████████████████████
467: sizeof() on Pointer Type	ME	8	████████████████████
477: Use of Obsolete Function	FN	7	████████████████████
401: Missing Release of Mem.	ME	6	████████████████████
476: NULL Pointer Dereference	ME	5	████████████████████
190: Integer Overflow	ME	5	████████████████████
783: Operator Precedence Error	EV	5	████████████████████
685: Func. Call Incorr. Num. of Args.	FN	4	████████████████████
768: Incorr.Short Circuit Evaluation	EV	4	████████████████████
252: Unchecked Return Value	FN	3	████████████████████
704: Incorr. Type Conversion/Cast	CN	3	████████████████████
682: Incorrect Calculation	CA	3	████████████████████
664: Impropr. Control of a Resource	RE	2	████████████████████
672: Op. on Resource after Expir.	RE	1	████████████████████
762: Mismatched Mem. Mgmt	ME	1	████████████████████
590: Free of Mem. not on the Heap	ME	1	████████████████████
687: Func. Call Incorr. Spec. Arg. Val	FN	1	████████████████████
683: Func. Call Incorr. Order of Args	FN	1	████████████████████
628: Func. Call Incorr. Spec. Args	FN	1	████████████████████
195: Signed to Unsigned Con. Error	CN	1	████████████████████
369: Divide By Zero	CA	1	████████████████████

Table 5: Distribution of code snippets with weaknesses introduced pre and post edits, and code snippets improved after revisions by weakness category

CWE Category	#VCS	%Introduced Pre- vs Post-Edit
CWE 398	520	████████████████████
Evaluation	124	████████████████████
Function	96	████████████████████
Memory	86	████████████████████
Initialization	75	████████████████████
Reachability	33	████████████████████
Calculation	4	████████████████████
Conversion	5	████████████████████
Resource	3	████████████████████

Summary of RQ2: We detect a total of 31 CWE types in 740 vulnerable code snippets (1221 CWE instances in total). These CWE types were generalized into 8 categories, and we find that evaluation, memory, and initialization weaknesses are the most common. Across all categories, vulnerabilities are more frequently introduced before revisions are made to the snippet.

Table 6: Revision types and their definitions

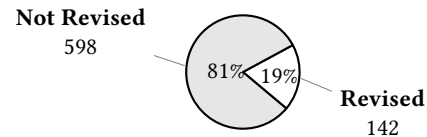
Revision Type	Definition
Code Correction CR	Changes to the syntax, and typo changes in comments and variable/function names.
Code Formatting FM	Adding white space or newlines, improving the formatting/readability of the code.
Code Improvement IP	Functionality or performance changes to the code, includes changes to logical expressions, calculations, and the types of variables or return values.
Code Removal / Addition RA	Removing or adding code segments, for example adding a new function or class.

4.3 RQ₃ Does the type of vulnerability differ depending on revision types?

4.3.1 Motivation. Users revise their answers for a variety of reasons. We aim to better understand the behaviour of these users by analyzing the types of revisions that are more commonly made when editing code snippets.

4.3.2 Approach. We manually analyze code snippets that have at least one code revision by looking at the nature of the edit. Then following work by Wang et al. [41], we label each revision with four revision types: code correction, code formatting, code improvement, and code removal/addition.

4.3.3 Results. An overview of the 4 revision types we label the revised code snippets as is shown in Table 6. Overall we find that 142 out of the 740 vulnerable code snippets are revised, as shown in Figure 7. Out of the 598 vulnerable code snippets that did not have any code revisions, 327 originate from posts that were never revised, meaning the user did not make any changes to the original version of the post. The remaining 271 code snippets were not revised, but rather were part of posts that were only textually edited. For example, users edit posts to correct typos, clarify their work, or to include references and links to other resources. For the 142 code snippets that were revised, we observe that users more frequently make revisions with the intention of improving the functionality of the example to better answer the question (86 out of 142 snippets, 60.6%), and to make corrections in the code such as fixing syntax errors and typos (31 out of 142, 21.8%). As shown in Figure 8, the least common type of edit we observe in the code snippets with revisions is formatting changes, such as adding white space through indentation (9 out of 142 code snippets).

**Figure 7: Number of code snippets revised and not revised**

We then further analyze the relationship between the CWE type present in a revised code snippet and its revision type. Table 7 shows

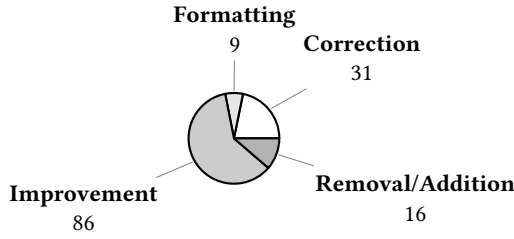


Figure 8: Distribution of revised vulnerable code snippets (VCS) by their revision type

Table 7: Distribution of revised code snippets by their revision type and type of weakness (Revision Types from Table 6 CR = Black, FM = Blue, IP = Magenta, RA = Green). #TV = Total Vulnerable Code Snippet VCS, #RV = Revised VCS. Cat. = CWE categories from Figure 6

Cat.	#TV	#RV	% Distribution of Revised VCS By Type			
Function	49	16	6.3	18.8	75.0	0
Memory	65	12	8.3	16.7	66.7	8.3
Evaluation	86	15	20.0	13.3	60.0	6.7
Initialization	59	13	23.1	7.7	69.2	0
Reachability	24	4	50.0	0	50.0	0
Resource	3	1	100.0	0	0	0

that across the 6/8 weakness categories that contain vulnerable code snippets that were revised, the most common revision type is code improvement. We also find that code correction revisions are more common in snippets with evaluation and initialization weaknesses (3 and 4 snippets respectively), and code removal/addition revisions are more common in snippets with memory weaknesses (5 snippets). Overall, there is a statistically significant difference between the number of vulnerable code snippets and the number of revised vulnerable code snippets across the six categories (Mann Whitney U test $p = 0.02$).

Summary of RQ3: We observe that out of the 142 code snippets that are revised, the most common types of revisions made are code improvements and code corrections. When looking at the relationship between CWE categories and revision types, we find that for the majority of CWE categories (6/8), code improvement revisions are the most common.

4.4 RQ₄ Were the vulnerabilities introduced pre-edit mitigated via post revisions?

4.4.1 Motivation. Revisions made by stack exchange users can improve code snippets by fixing errors and reducing vulnerabilities, or they can further deteriorate an already vulnerable snippet by adding new weaknesses. Revisions may also leave vulnerabilities unchanged. It is thus important to better understand the impact of code revisions on reducing vulnerabilities.

4.4.2 Approach. Using the version history of the obtained code snippets, we first determine the number of code revisions for each

code snippet. For the snippets that have at least one revision, we run all versions through cppcheck to determine if the number of vulnerabilities stayed the same, decreased, or increased.

4.4.3 Results. We look at whether certain revision types are correlated more closely with particular revision outcomes, such as reducing the number of vulnerabilities in the snippet or introducing new ones. As shown in Fig 9, for the 40 revised code snippets that contained correction and formatting revisions, all did not experience any change in vulnerabilities. We further find that all 9 code snippets that were improved due to revisions were revised with the intent to improve the code, such as Listing 3. However, a large number of code snippets with improvement related revisions also experienced deterioration or no change in the number of vulnerabilities (23 and 54 code snippets respectively). Finally, we notice that code snippets with revisions related to the removal or addition of large segments of code were more likely to deteriorate (12 out of 16 snippets). This is likely due to the fact that the addition of large code segments increases the chance of introducing a weakness. For example, in the following Stack Overflow answer ([A52560467](#)), the user revised the snippet by adding the `check_relay` function and the large switch statement in the `enable_relay` function. Although these changes may have been made with the intention of better answering the question, they ultimately introduced an instance of CWE 398 in line 35 due to the scope of the variable state.

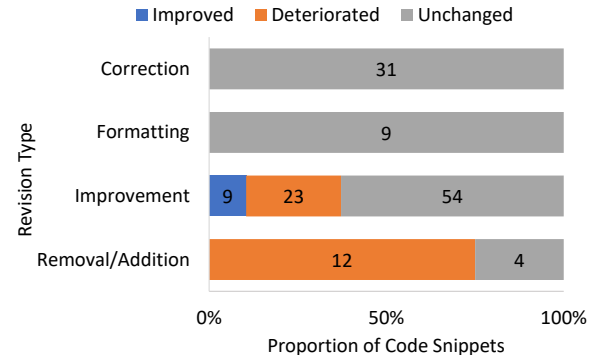


Figure 9: Distribution of revision effect (improved, deteriorated, or unchanged) by revision type

Overall, only a small number of code snippets experienced an improvement due to revisions (9 in total). As shown in Figure 10, those with initialization related weaknesses and instances of CWE 398 contained the most (2 out of 59, and 5 out of 520 respectively).

In total, 115 code snippets with pre-existing vulnerabilities experienced one or more revisions. In Figure 11, we observe that the majority of all revised code snippets (in total 142) were revised just once. However, we also observe that the effect of revisions on these code snippets is minimal. Figure 12 shows the vast majority of these code snippets with pre-existing vulnerabilities that were revised did not experience a decrease or increase in vulnerabilities (98 out of 115). We also find that in some code snippets (9 out of 115), revisions removed vulnerabilities that existed in previous versions. However, in a similar number of code snippets (8 out of 115), vulnerabilities were introduced by revisions.



Figure 10: Distribution of code snippets that were improved due to revisions by CWE type or CWE category

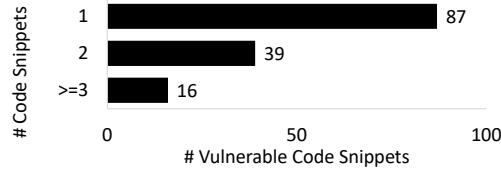


Figure 11: Distribution of the number of code revisions

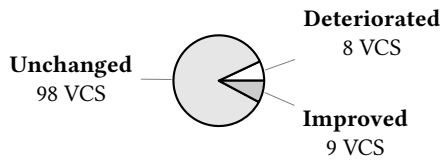


Figure 12: Distribution of revision effect in snippets with pre-existing vulnerabilities

Stack Overflow answer *A25827521* is an example of a snippet that was revised once but did not improve in terms of removing its weakness. By comparing the final version of the code to the original, we observe that the user likely intended to improve the functionality and correctness of the code. We see they changed the function parameters to void instead of leaving it empty to ensure no arguments could be passed, and they also attempted error handling by first checking if `read_AT_string` did not return NULL. However, they did not address the instance of CWE 562 - Return of Stack Variable Address detected by `cppcheck` in line 36 where the return value was a pointer to a local variable, which is invalid in C++. This is an example of a revision that went beyond non-functional changes such as adding comments or fixing typos, but was still not effective at removing the weakness in the snippet.

We analyze the 31 deteriorated code snippets for similarities in the changes made to the code, and the subsequent CWE instances that were introduced. In total, we find 4 distinct deterioration types: (1) New component added + introduced new weakness, (2) Modified existing component + introduced new weakness, (3) New component added + introduced more existing weaknesses, and (4) Modified existing component + introduced more existing weaknesses. We further find that a few deteriorations occurred due to the user fixing a syntax error in the code, which allowed for more weaknesses to be detected by `cppcheck` (5). The distribution of these 5 types is shown in Figure 13, where we see that the most common type of deterioration was caused by users modifying an existing

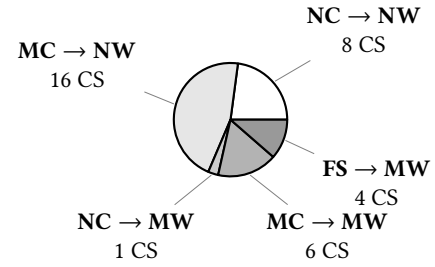


Figure 13: Distribution of deterioration type (M = Modified, N = New, C = Code, W = Weakness. FS = Fixed Syntax.)

component in the code (such as a function, variable, or class), and introducing new CWE instances that were not present before.

Summary of RQ4: The vast majority of revised snippets remained unchanged in terms of the number of CWE instances present in the code. When looking at the effect of each revision type, we find that all revised related to code correction and formatting left the code snippet unchanged, while a large proportion of code removal/addition type revisions deteriorated.

5 DISCUSSION

Our study findings can guide the following stakeholders: IoT developers, IoT vendors, Forum designers, and IoT researchers and educators. We discuss the implications below.

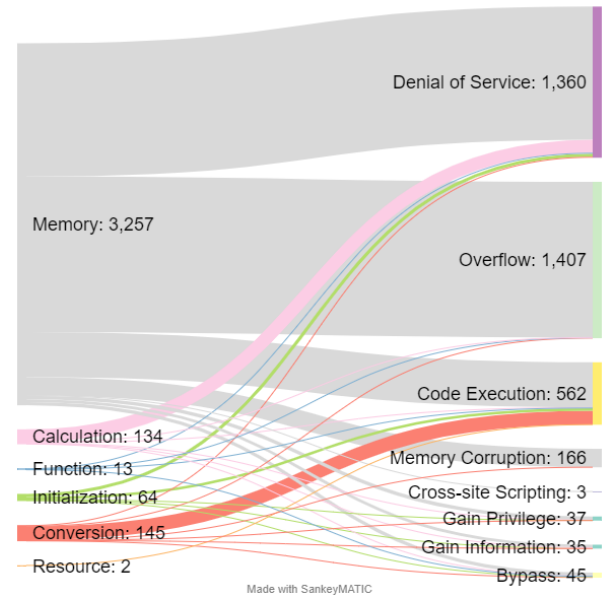


Figure 14: Mapping of CWE categories to CVE Types. Width of each line represents the number of CVEs per CWEs.

IoT Developers: In Figure 14, we show the number of CVEs reported in the NVD database per the six vulnerability types we

observed in our IoT code snippets (in pre + post revisions). The reported CVEs are grouped under eight types in the cvedetails.com site: (1) Denial of service, (2) Overflow, (3) Code execution, (4) Memory corruption, (5) Cross-site scripting, (6) Gain privilege, (7) Gain information, and (8) Bypass. This Figure 14 shows that the six vulnerability types in the IoT code snippets can cause all the eight types of critical security issues in the IoT devices, if the vulnerable code snippets are reused from the Stack Exchange sites. Therefore, IoT developers need to stay aware of the potential security problems in such shared code snippets in the developer forums. Our study findings like the catalog of CWEs and the associated vulnerable code snippets can be used by the IoT developers to learn about such pitfalls. Such knowledge can be useful for the developers in multiple phases. First, when they share any IoT code examples in the forums. Second, when they revise a shared code example. Third, when they reuse a shared code example. In all phases, they can check the code for vulnerability by consulting our catalog of CWEs. Given that revisions from others rarely fix such a vulnerable code snippets, it is important for the IoT developers to practice such quality assurance of the code snippets, even after the code snippet is revised by other users in the forums.

IoT Vendors: In Figure 14, we showed that the six vulnerability type we observed in the shared IoT code snippets can be mapped to eight CVE types in NVD database. In the NVD database, each reported CVE is categorized into the severity types: Critical (C), High (H), Medium (M), and Low (L). In Table 8, we show the distribution of the CVEs by four severity types. Overall, we see that all six vulnerability categories in our observed IoT code snippets can contribute to many critical and highly severe security vulnerabilities in the IoT devices. In Figure 5, we showed that such affected IoT devices can belong to many vendors (e.g., Cisco, Snapdragon, etc.). Therefore, IoT device and SDK vendors can work together to make the devices more resilient. One solution would be to incorporate automated security testing tool into the IoT SDKs and devices. The IoT vendors cannot rely much on the collaborative editing system in the crowd-sourced developer forums to improve the code snippets.

Table 8: Distribution of the 12 CWEs with mapped CVEs in the cvedetails.com database. Each colored bar under CVSS score category denotes a severity category (Black = Low, Cyan = Medium, Magenta = High, Red = Critical)

CWE Category	#CVEs	%Distribution by CVSS Score Category
Memory	3460	%L %M %H %C
Calculation	276	%L %M %H %C
Conversion	172	%L %M %H %C
Initialization	172	%L %M %H %C
Function	39	%L %M %H %C
Resource	17	%L %M %H %C
Overall	4136	%L %M %H %C

Forum Designers: In Table 9, we show the distribution of our observed six vulnerability types across the four types of code revisions we observed, i.e., whether and how a revision type introduced a vulnerability type in the revised code. We find that correction to a code introduced all the six types of vulnerability categories. Intuitively, this observation goes against the general assumption

Table 9: Distribution of weakness categories by revision type. Each colored bar denotes a different category. (Black = Function, Green = Memory, Magenta = Evaluation, Red = Initialization, Cyan = Reachability, Orange = Resource)

CVE Type	# Code Snippets per Category
Correction	Black Green Magenta Red Cyan Orange
Formatting	Black Green Magenta Red Cyan Orange
Improvement	Black Green Magenta Red Cyan Orange
Removal/Addition	Black Green Magenta Red Cyan Orange

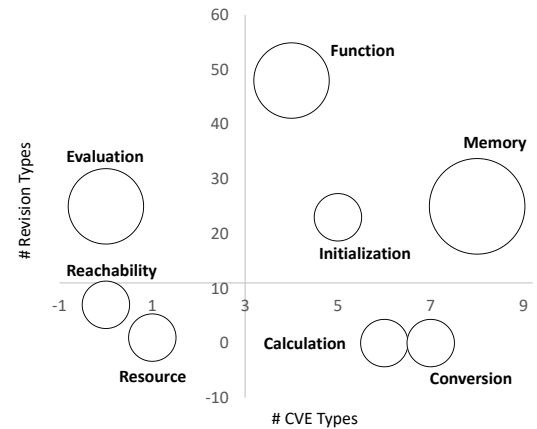


Figure 15: The tradeoff between the revisions and the vulnerabilities introduced towards the IoT code snippets

that correction to a code should have fixed more vulnerability. The statistics from Table 9 can inform forum designers of the fact that the current mechanisms (e.g., the four revision types) to support collaborative editing in the online forums are insufficient to help mitigate security vulnerabilities in the shared code. In Figure 15, we reinforce this observation by showing a bubble chart as a tradeoff between the number of revisions made to our studied vulnerable code snippets and the number of distinct CVE types that were introduced during the revisions. The size of each bubble corresponds to the number of total CVEs reported against the CWE IDs found per CVE category. Figure 15 shows that the most number of CVEs reported for the ‘Memory’ category weaknesses, and code snippets with such weaknesses in our dataset were revised considerably with little or no success in fixing. On the other hand, code snippets belonging to ‘Conversion’ type weaknesses were revised almost never. Overall, there is a positive correlation between the number of revisions made to a code snippet and the number of vulnerabilities found in the code snippet. The findings call for a redesign in the collaborative editing process in the forums by the designers of the sites, e.g., to facilitate the incorporation of security guidelines into the editing process by providing automated recommendations.

IoT Researchers and Educators: Our findings offer a grim picture on the effectiveness of collaborative editing to help mitigate security vulnerabilities in developer forums. IoT researchers can join hands with both the forum designers and the IoT vendors to

conduct research on the better design of the collaborative editing and to incorporate security validation framework into the IoT devices. Our findings reinforce the recent worries on software supply chain attacks [27] by showing that security vulnerabilities are prevalent in online developer forums and they are mostly left unaddressed during revisions. One way to help IoT developers during the sharing of code snippets in online forums is to educate them with on-demand documentation about the security issues by consulting security patterns and the vulnerabilities reported in the NVD database. The IoT security educators can join hands with the forum designers to produce such documentation, which can also offer new directions to the current approaches that utilize online developer forums to create and/or improve software documentation [8, 34–38]. This is important given studies that IoT developers do indeed consult about security issues in online developer forums [33], but they also face difficulty to get answers to their questions [39].

6 THREATS TO VALIDITY

Internal validity threats relate to author bias in deciding which weaknesses to ignore. We noticed that some claimed weaknesses in cppcheck were not accurate. We addressed this issue by suppressing certain CWE types in Cppcheck like CWE 563 (Assignment to Variable without Use) and by following a previous study [42] to suppress syntax errors and to ignore code snippets with less than 5 lines. In addition, the categorization of the 28 distinct CWE types into 8 weakness categories was done by both authors. **Construct validity** threats relate to errors that may have occurred during the data collection. To determine if a SO post was related to IoT, we used tags from existing studies [33, 39]. For Arduino and Raspberry, we made the assumption that all posts would be related to IoT. Another threat is our use of the language detection tool guesslang to identify C/C++ code snippets. Guesslang has been used in previous studies to specifically detect C/C++ code and has a validity rate of 90% [14]. **External validity** threats relate to how our findings can be generalized to the nature of IoT posts on online Q/A sites as a whole. We focused on vulnerabilities in Stack Exchange answers. This is because code snippets found in answers are meant to be ‘solutions’ and are more likely to be copied and used by developers. We also focus our study on strictly C and C++ code snippets due to their popularity in IoT development.

7 RELATED WORK

To the best of our understanding, the C/C++ code examples shared in Stack Overflow were subject to two empirical studies recently, first by Verdi et al. [40] and then by Zhang et al. [42]. Our study differs from the two studies as follows.

- (1) While both Verdi et al. [40] and Zhang et al. [42] analyze C/C++ code examples in general, we focused on IoT C/C++ code examples. While both analyzed only SO code examples, we studied data from three sites: SO, Arduino, and Raspberry Pi.
- (2) While Verdi et al. [40] analyzed C/C++ code for weakness, we studied revisions to the vulnerable C/C++ IoT code.
- (3) Unlike Verdi et al. [42] and Zhang et al. [42], we studied the vulnerability types and their relationships with different revision types. Our focus is to learn whether and how revisions could help mitigate the observed vulnerability types.

We observed some similarities and differences between our study results and above two papers. First, in all SO C/C++ code snippets, Zhang et al., found 32 CWE types [42] while Verdi et al. found 31 CWE types [40]. We found 28 distinct CWE types identified in the IoT C/C++ code snippets. Zhang et al., who similar to us used cppcheck to automatically detect CWE instances, found that 1.82% of their collected code snippets (11,748 out of 646,716) contained weaknesses. However, we observed a slightly higher proportion for IoT code examples as having at least one CWE (6.4%). Verdi et al. manually reviewed all of their 72,483 code snippets. They found vulnerabilities in 99 (i.e., 0.14%) of their SO code snippets.

Other related work can be broadly divided into **Studies** and **Techniques** to understand and mitigate IoT security issues.

Studies investigated underlying middleware solutions [9], big data analytics [21], and the design of secure protocols and techniques [2, 19, 43] and their applications on diverse domains (e.g., eHealth [22]). SO posts have been previously studied for insecure python vulnerabilities [28], topics discussed by IoT developers [20, 33, 39], big data [4] and chatbot issues [1]. **Techniques** and safety measures are studied in Soteria [6], IoTGuard [7]. IoT devices can be easy targets for cyber threats [12, 43]. Encryption and secure hashing technologies [31]. Many authorization techniques for IoT are proposed like SmartAuth [32]. For smart home security, IoT security techniques are proposed like Piano [13], smart authentication [16], and cross-App Interference threat mitigation [10]. Attacks on Zigbee, an IEEE specification used to support interoperability can make IoT devices vulnerable [29]. We are not aware of any studies that checked the effectiveness of revisions to help mitigate vulnerabilities in online shared code.

8 CONCLUSION

We analyzed code examples from the Stack Overflow, Arduino, and Raspberry Stack Exchange sites. We focused on analyzing weaknesses by analyzing their revision history. We found a total of 31 CWE types present in 740 code snippets. We observed that the vast majority of vulnerabilities are introduced pre code revisions (713 out of 740). When snippets are revised, the number of vulnerabilities that are present in that snippets are likely to not change. Our results indicate the collaborative editing in the forums do not help mitigate the code vulnerabilities. Our future work will focus developing techniques to incorporate security recommendations into the collaborative editing process.

REFERENCES

- [1] Ahmad Abdellatif, Diego Costa, Khaled Badran, Rabe Abdalkareem, and Emad Shihab. 2020. Challenges in Chatbot Development: A Study of Stack Overflow Posts. In *17th International Conference on Mining Software Repositories, October 5–6, 2020, Seoul, Republic of Korea*. New York, NY, USA. ACM.
- [2] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials* 17, 4 (2015), 2347–2376.
- [3] Andrei Arusoae, Stefan Ciobaca, Vlad Craciun, Dragos Gavrilut, and Dorel Lucanu. 2017. A Comparison of Open-Source Static Analysis Tools for Vulnerability Detection in C/C++ Code. 161–168. <https://doi.org/10.1109/SYNASC.2017.00035>
- [4] Mehdi Bagherzadeh and Raffi Khatchadourian. 2019. Going Big: A Large-scale Study on What Big Data Developers Ask. In *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (Tallinn, Estonia) (ESEC/FSE 2019)*. ACM, New York, NY, USA, 432–442.

- [5] Sebastian Baltes, Lorik Dumani, Christoph Treude, and Stephan Diehl. 2018. SOTorrent: Reconstructing and Analyzing the Evolution of Stack Overflow Posts. *Proceedings of the 15th International Conference on Mining Software Repositories* (May 2018), 8. <https://doi.org/10.1145/3196398.3196430>
- [6] Z Berkay Celik, Patrick Drew McDaniel, and Gang Tan. 2018. SOTERIA: automated IoT safety and security analysis. In *USENIX Conference on Usenix Annual Technical Conference*. 147 – 158.
- [7] Z Berkay Celik, Gang Tan, and Patrick Drew McDaniel. 2019. IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT. In *Network and Distributed System Security Symposium*. 15.
- [8] Partha Chakraborty, Rifat Shahriyar, Anindya Iqbal, and Gias Uddin. 2021. How Do Developers Discuss and Support New Programming Languages in Technical Q&A Site? An Empirical Study of Go, Swift, and Rust in Stack Overflow. *Information and Software Technology (IST)* (2021), 19.
- [9] Moumena A Chaqfeh and Nader Mohamed. 2012. Challenges in middleware solutions for the internet of things. In *International Conference on Collaboration Technologies and Systems (CTS)*. 21–26.
- [10] Haotian Chi, Qiang Zeng, Xiaojiang Du, and Jiaping Yu. 2020. Cross-App Interference Threats in Smart Homes: Categorization, Detection and Handling. In *50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. 411–423.
- [11] Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl. 2017. Stack overflow considered harmful? the impact of copy&paste on android application security. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 121–136.
- [12] Mario Frustaci, Pasquale Pace, Gianluca Aloï, and Giancarlo Fortino. 2017. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal* 5, 4 (2017), 2483 – 2495.
- [13] Neil Zhenqiang Gong, Altay Ozen, Yu Wu, Xiaoyu Cao, Richard Shin, Dawn Song, Hongxia Jin, and Xuan Bao. 2017. PIANO: Proximity-Based User Authentication on Voice-Powered Internet-of-Things Devices. In *37th International Conference on Distributed Computing Systems*. 2212 – 2219.
- [14] GuessLang. n.d. Guesslang documentation. [https://guesslang.readthedocs.io/en/latest/#:\\$sim\\$.text=Guesslang%20detects%20the%20programming%20language,a%20million%20source%20code%20files](https://guesslang.readthedocs.io/en/latest/#:sim.text=Guesslang%20detects%20the%20programming%20language,a%20million%20source%20code%20files). Accessed: 2021-11-23.
- [15] Fraser Hall, Leandros Maglaras, Theodoros Aivaliotis, Loukas Xagoraris, and Ioanna Kantzavelou. 2020. Smart Homes: Security Challenges and Privacy Concerns. (10 2020), 1–3.
- [16] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlene Fernandes, and Blase Ur. 2018. Rethinking access control and authentication for the home internet of things (IoT). In *27th USENIX Conference on Security Symposium*. 255 – 272.
- [17] AbdelRahman Hussein. 2019. Internet of Things (IOT): Research Challenges and Future Applications. *International Journal of Advanced Computer Science and Applications* 10 (01 2019), 77. <https://doi.org/10.14569/IJACSA.2019.0100611>
- [18] Iman Keivanloo, Juergen Rilling, and Ying Zou. 2014. Spotting working code examples. (05 2014), 7. <https://doi.org/10.1145/2568225.2568292>
- [19] Minhaj Ahmad Khan and Khaled Salah. 2018. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems* 82 (2018), 395–411.
- [20] Nibir Mandal and Gias Uddin. 2022. An Empirical Study of IoT Security Aspects at Sentence-Level in Developer Textual Discussions. *Elsevier Information and Software Technology* 50 (2022).
- [21] Mohsen Marjani, Fariza Nasaruddin, Abdullah Gani, Ahmad Karim, Ibrahim Abaker Targio Hashem, Aisha Siddiqua, and Ibrar Yaqoob. 2017. Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. *IEEE Access* 5, 1 (2017), 5247 – 5261.
- [22] Daniel Minoli, Kazem Sohraby, and Benedict Occhiogrosso. 2017. IoT Security (IoTSec) Mechanisms for e-Health and Ambient Assisted Living Applications. In *IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*. 13–18.
- [23] MITRE. 2021. CWE VIEW: Weaknesses in Software Written in C. Accessed: 2021-11-10.
- [24] MITRE. 2021. CWE VIEW: Weaknesses in Software Written in C++. Accessed: 2021-11-10.
- [25] MITRE. n.d. About CWE. <https://cwe.mitre.org/about/index.html> Accessed: 2021-10-18.
- [26] MITRE. n.d. CWE List Version 4.6. Accessed: 2021-11-2.
- [27] National Institute of Standards and Technology. 2021. Defending Against Software Supply Chain Attacks. https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf. [Online; accessed 1-May-2022].
- [28] Akond Rahman, Effat Farhana, and Nasif Imtiaz. 2019. Snakes in paradise?: insecure python-related coding practices in stack overflow. In *Proceedings of the 16th Working Conference on Mining Software Repositories*. IEEE / ACM, 200–204. <https://doi.org/10.1109/MSR.2019.00040>
- [29] Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn. 2017. IoT goes nuclear: Creating a ZigBee chain reaction. In *IEEE Symposium on Security and Privacy*. 195 – 212.
- [30] Satyajit Sinha. 2021. State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion. <https://iot-analytics.com/number-connected-iot-devices/>.
- [31] Pietro Tedeschi, Savio Sciancalepore, Areej Eliyan, and Roberto Di Pietro. 2020. LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications. *IEEE Internet of Things Journal* 7, 1 (2020), 621–638.
- [32] Yuan Tian, Ferdian Thung, Abhishek Sharma, and David Lo. 2017. APIBot: question answering bot for API documentation. In *Proc. 32nd IEEE/ACM International Conference on Automated Software Engineering*. 153–158.
- [33] Gias Uddin. 2021. Security and Machine Learning Adoption in IoT: A Preliminary Study of IoT Developer Discussions. [arXiv:2104.00634 \[cs.CR\]](https://arxiv.org/abs/2104.00634)
- [34] Gias Uddin and Foutse Khomh. 2017. Automatic Summarization of API Reviews. In *Proc. 32nd IEEE/ACM International Conference on Automated Software Engineering*. 12.
- [35] Gias Uddin and Foutse Khomh. 2019. Automatic Opinion Mining from API Reviews from Stack Overflow. *IEEE Transactions on Software Engineering* (2019), 35.
- [36] Gias Uddin, Foutse Khomh, and Chanchal K Roy. 2020. Automatic Mining of API Usage Scenarios from Stack Overflow. *Information and Software Technology (IST)* (2020), 16.
- [37] Gias Uddin and Martin P. Robillard. 2015. How API Documentation Fails. *IEEE Software* 32, 4 (2015), 76–83.
- [38] Gias Uddin and Martin P. Robillard. 2017. *Resolving API mentions in informal documents*. Technical Report. McGill University.
- [39] Gias Uddin, Fatima Sabir, Yann-Gaël Guéhéneuc, Omar Alam, and Foutse Khomh. 2021. An Empirical Study of IoT Topics in IoT Developer Discussions on Stack Overflow. *Empirical Software Engineering* 26, 121 (2021).
- [40] M. Verdi, A. Sami, J. Akhondali, F. Khomh, G. Uddin, and A. Karami Motlagh. 5555. An Empirical Study of C++ Vulnerabilities in Crowd-Sourced Code Examples. *IEEE Transactions on Software Engineering* 01 (sep 5555), 1–19. <https://doi.org/10.1109/TSE.2020.3023664>
- [41] Yuhao Wu, Shaowei Wang, Cor-Paul Bezemer, and Katsuro Inoue. 2019. How Do Developers Utilize Source Code from Stack Overflow? *Empirical Software Engineering* 24 (04 2019), 2. <https://doi.org/10.1007/s10664-018-9634-5>
- [42] Haoxiang Zhang, Shaowei Wang, Heng Li, Tse-Hsun Peter Chen, and Ahmed E. Hassan. 2021. A Study of C/C++ Code Weaknesses on Stack Overflow. *IEEE Transactions on Software Engineering* PP (02 2021), 1–15. <https://doi.org/10.1109/TSE.2021.3058985>
- [43] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shihpyng Shieh. 2014. IoT Security: Ongoing Challenges and Research Opportunities. In *IEEE 7th International Conference on Service-Oriented Computing and Applications*. 230–234.