Poster: GlucOS: A secure, safe and extensible system for automated insulin delivery

Hari Venugopalan
hvenugopalan@ucdavis.edu
UC Davis

Shyreas Madhav Ambattur Vijayanand
smvijay@ucdavis.edu
UC Davis

Samuel T. King
kingst@ucdavis.edu
UC Davis

Abstract—Type 1 Diabetes (T1D) is a metabolic disorder where an individual’s pancreas stops producing insulin. To compensate, they inject synthetic insulin. The dynamics of insulin and the impact of various intrinsic and extraneous factors on glucose complicate the management of T1D [19]. While research has shown that modern machine learning (ML) based algorithms [19], [8], [18], [16] are well suited for managing T1D, existing automated insulin delivery systems [10], [13], [4], [2], [1] do not support ML.

Incorrect predictions from ML, either from a malicious model [6], [9] or from the blind spots of a benign model, can kill people when used to control an insulin pump. Automated insulin delivery systems also have to contend with other practical challenges in the real world such as skin infections [12] and pump failures [7]. These risks along with the lack of explainability of complex ML discourages people from adopting ML in practice to manage T1D [3].

Thus, current system builders and users opt for explainable and deterministic algorithms that offer modest control in managing T1D over the most accurate predictions from state-of-the-art ML. However, people living with T1D miss out on a viable opportunity to improve their long-term health and reduce their T1D management burden by not using using ML.

In this paper, we take on the challenge of supporting powerful predictive ML algorithms for managing T1D. We build the first automated insulin delivery system that can adopt any algorithm to control an insulin pump securely and safely. Our contribution is in our novel system, called GlucOS, that we design and implement from scratch, and in our novel security mechanisms that handle both security and safety when automatically dosing insulin. GlucOS is not tied to any specific algorithm and can safely support any algorithm, including ML-based [20], [15], physiological-based [5], [17], control theoretic [11], [14], and heuristic-based [13], [10].

Our key insight for security is that over a long enough period of time, all correct algorithms will dose the same amount of insulin. For example, on a given day, a person will need to dose a fixed amount of insulin to absorb all of the glucose from the food they eat. Since synthetic insulin action is slow, predicting future metabolic states to inject insulin early is critical for long-term health. GlucOS’s support for modern ML-based algorithms provides users with this predictive power to dose insulin. For security, GlucOS pairs a predictive ML model with a conservative and safe model to provide the ML with enough flexibility to control the insulin pump proactively while staying within the bounds dictated by the safe model.

Rather than throw away the boring old traditional algorithms that current systems use and replacing them with fancy ML, we repurpose these simple algorithms to serve as the foundation for our security logic. By grounding our security logic in easy to understand and effective algorithms, we inherit the explainability and determinism that come with them.

We report our experiences running GlucOS on one individual for 2.5 months to manage their T1D. Running our software on a real human forces us to design a practical and real system. Our evaluation using virtual humans in a simulator show that our security and safety mechanisms generalize beyond the specific individual.

Our novel contributions include:

• The clean-slate design and implementation of a flexible automated insulin delivery system that supports any predictive algorithm to manage T1D safely.
• Security mechanisms grounded by safe physiological models that protect individuals from egregious errors and malicious predictions.
• A case study describing our experiences from a real-world deployment, and results from simulation to show that our techniques generalize.

REFERENCES


GlucOS: A secure, safe and extensible system for automated insulin delivery

Hari Venugopalan, Shreyas Madhav Ambattur Vijayanand and Samuel T King
University of California, Davis

Problem Statement

● ML based algorithms are well suited for managing Type 1 Diabetes (T1D).
  ○ Calculating insulin doses depends on various intrinsic and extraneous factors.
  ○ ML can predict insulin dynamics.
  ○ Millions of papers published on using ML to manage T1D.

● Automated insulin delivery systems do not use ML.
  ○ Incorrect ML predictions can kill individuals.
  ○ Looser control and long-term health complications.

● GlucOS to the rescue:
  ○ Extensible: GlucOS supports any algorithm for automated insulin delivery, ML or otherwise.
  ○ Safe and Secure: GlucOS repurposes traditional algorithms to provide the foundation for security.
  ○ Allows ML to be proactive with insulin delivery while staying within the bounds of traditional algorithms for safety and security.

System Design

Real-world Deployment

<table>
<thead>
<tr>
<th>Glucose Range (mg/dl)</th>
<th>Range label</th>
<th>Reactive Model</th>
<th>Predictive ML Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;54</td>
<td>L2 Hypo</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>54-69</td>
<td>L1 Hypo</td>
<td>0.48%</td>
<td>0%</td>
</tr>
<tr>
<td>70-180</td>
<td>In range</td>
<td>91.9%</td>
<td>97.22%</td>
</tr>
<tr>
<td>181-250</td>
<td>L1 Hyper</td>
<td>7.62%</td>
<td>2.78%</td>
</tr>
<tr>
<td>&gt;250</td>
<td>L2 Hyper</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Results

Malicious algorithm dosing 10x the required insulin without GlucOS (instant death)

Malicious algorithm dosing 0.1x the required insulin without GlucOS (health complications)

Malicious algorithm dosing 10x the required insulin with GlucOS

Malicious algorithm dosing 0.1x the required insulin with GlucOS

Future Work

● Authentication: Repurpose insulin delivery systems to provide seamless authentication for individuals with T1D.
● Formal Verification: Prove safety from implementational vulnerabilities/bugs.
● HCI: Discover effective alerting methods for individuals who prefer manual injections.